FortiSandbox - AWS Guide

Version 2.5.0

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

January 05, 2018
FortiSandbox 2.5.0 AWS Guide
34-250-465480-20180105

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-05	Initial release.

Introduction

Fortinet's FortiSandbox on AWS enables organizations to defend against advanced threats in the cloud. It works alongside network, email, endpoint, and other security measures, or as an extension of on-premises security architectures to leverage scale with complete control.

FortiSandbox Amazon Machine Image is available on the AWS Marketplace. This guide provides users with an easy-to-follow, step-by-step guide for successful deployment.

FortiSandbox on AWS can be installed as a standalone zero-day threat prevention or it can work in conjunction with your existing FortiGate, FortiMail, or FortiWeb AWS instances to identify malicious and suspicious files, ransomware, and network threats.

What is FortiSandbox?

FortiSandbox uses a two-stage process to identify zero-day, advanced malware including ransomware, and generate relevant threat intelligence.

Stage 1:

Pre-filtering is performed by an engine powered by Fortinet's threat research and FortiGuard Labs Intelligence.

Stage 2:

Dynamic behavior analysis is performed on objects to determine if they are malicious. Rating verdicts are returned to the originating device in real-time to act upon within Fortinet Fabric security products, third-party vendor security products via JSON API, or as a feed via STIX format.

FortiSandbox on AWS Use Cases

Use Case 1: Instantaneous Indicators of Compromise (IOC) Intelligence Sharing Across Multi-Clouds

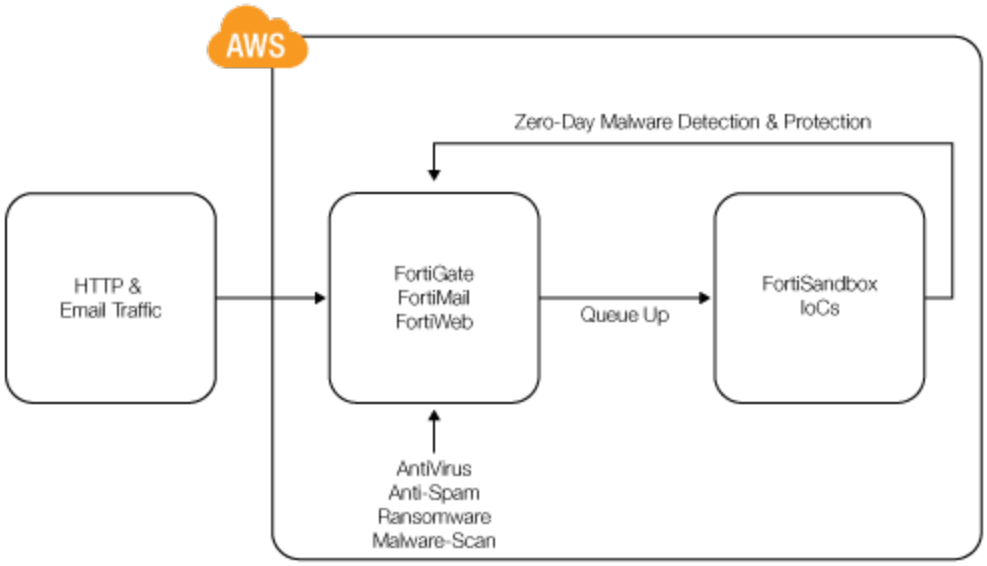
In hybrid or multi-cloud environments, it is critical to get first-hand IOC intelligence for zero-day malware protection. FortiSandbox instantly shares session information and IOC related to the malware behavior. If there are multiple FortiSandbox instances (physical, virtualized, or cloud) present, you can identify the synchronization rule for the intelligence update.

Use Case 2: Fabric-Based Deep Analysis for Zero-Day Malware Detection

FortiSandbox on AWS introduces elasticity for on-demand sandbox resources when they are needed, which can be very costly in the traditional on premises setting. When working with other Fortinet products like FortiGate, FortiWeb, or FortiMail, FortiSandbox continues to be a powerful use case for public cloud when no prior malware signature exists. When the firewall does not find the AV malicious profile in the HTTP or web traffic, it submits and queues the file sample in FortiSandbox on AWS for in-depth analysis until the verdict is reached.

Adaptive Notification and Remediation

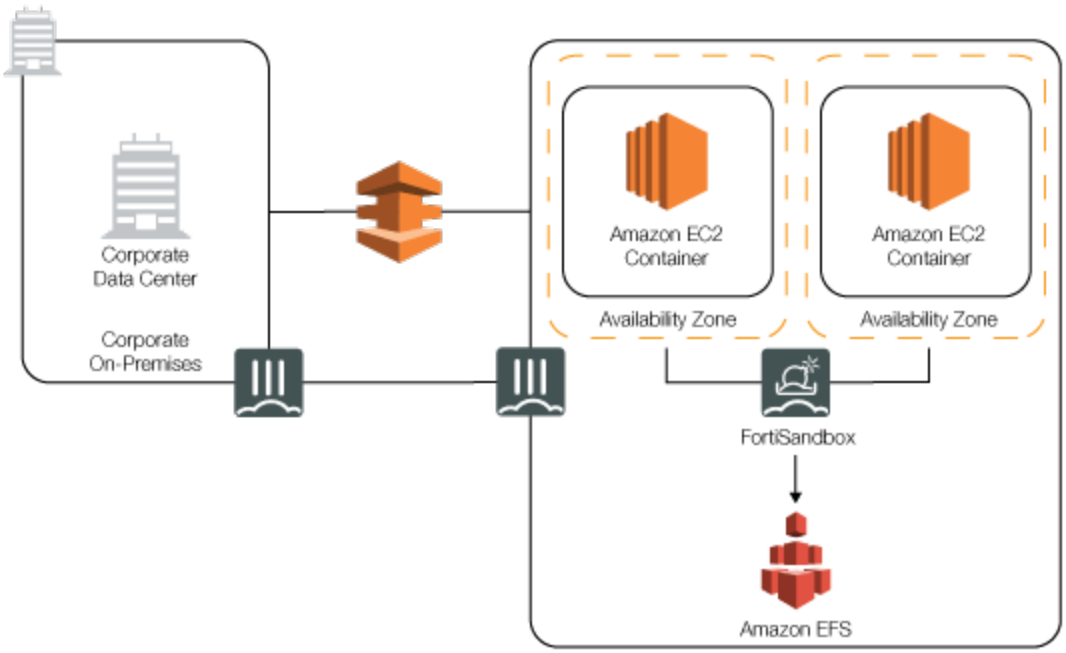
The intelligence is shared across the Fabric. Every signature and IOC that FortiSandbox generates is automatically propagated across all FortiGate firewalls and FortiClient endpoints for immediate blocking or quarantine actions to avoid further damage.



When anticipated traffic is down it can release the AWS compute resources if not needed.

Use Case 3: FortiSandbox Cloud Scan Automation

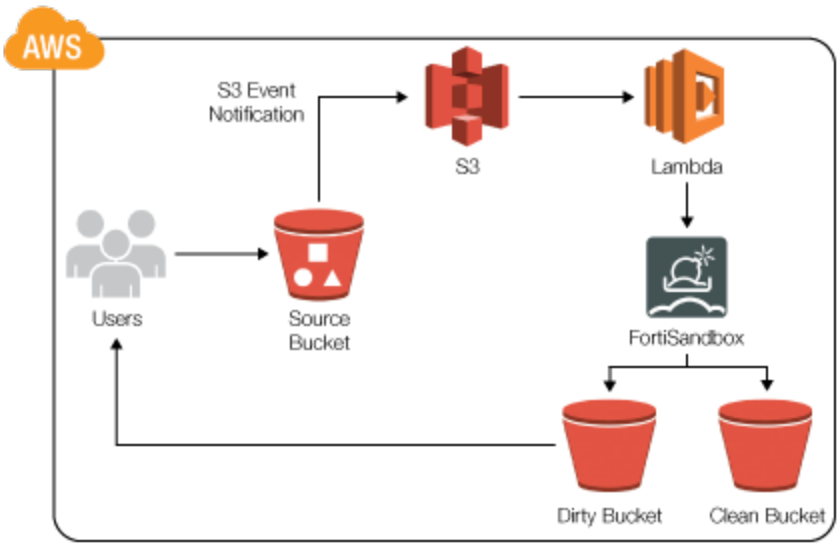
Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. EFS is used often in cloud migration such as dataset migration, on-demand backup or cloud bursting scenarios. You can mount your Amazon EFS file systems on your on-premises data center servers when connected to your Amazon VPC with AWS Direct Connect or through a FortiGate site-to-site secured connection. In the process, you can insert FortiSandbox on premises or in AWS, or you can perform malware analysis in the EFS-to-EFS backup solution to ensure clean file backup.



S3 Bucket Scanning

The other way to use FortiSandbox through NFS mount is to leverage AWS Storage Gateway. By mounting a file share and mapping it to an Amazon S3 bucket using AWS Storage Gateway, you can configure AWS S3 as the NFS or SMB network share for FortiSandbox malware analysis.

When used in conjunction with the Amazon S3 event notification feature, it enables you to receive notifications when certain file events occur in the bucket and use the AWS Lambda function to queue the file sample to FortiSandbox for malware analysis.

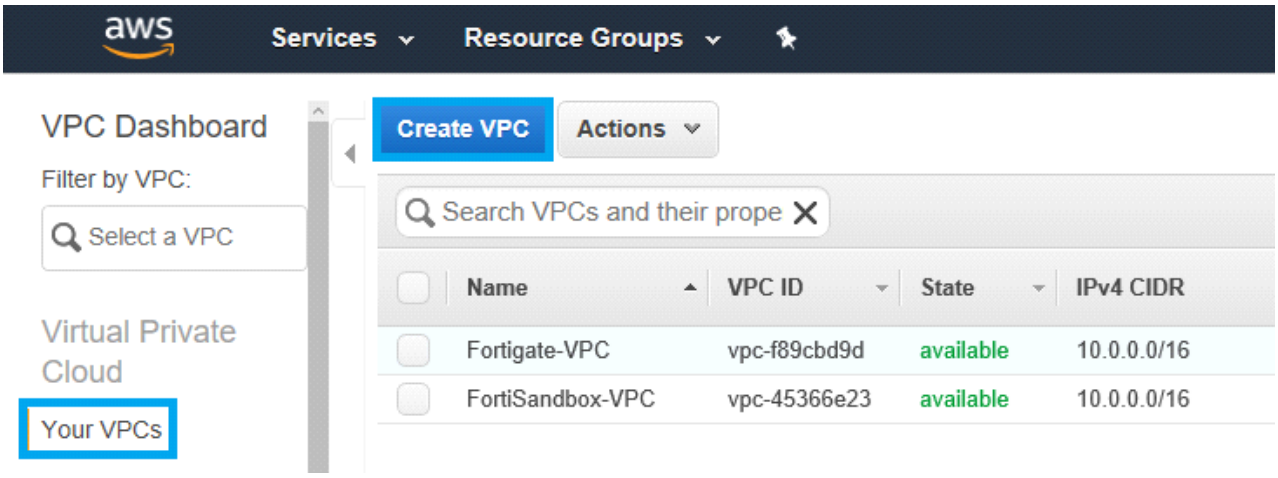


Other use cases such as preventing malware penetration in a closed/isolated network can be considered. Without any external malware signatures, FortiSandbox can help perform zero-day malware analysis instead. For more architecture discussion, please email aws@fortinet.com if you need to clarify the use cases.

Basic AWS Network Setup

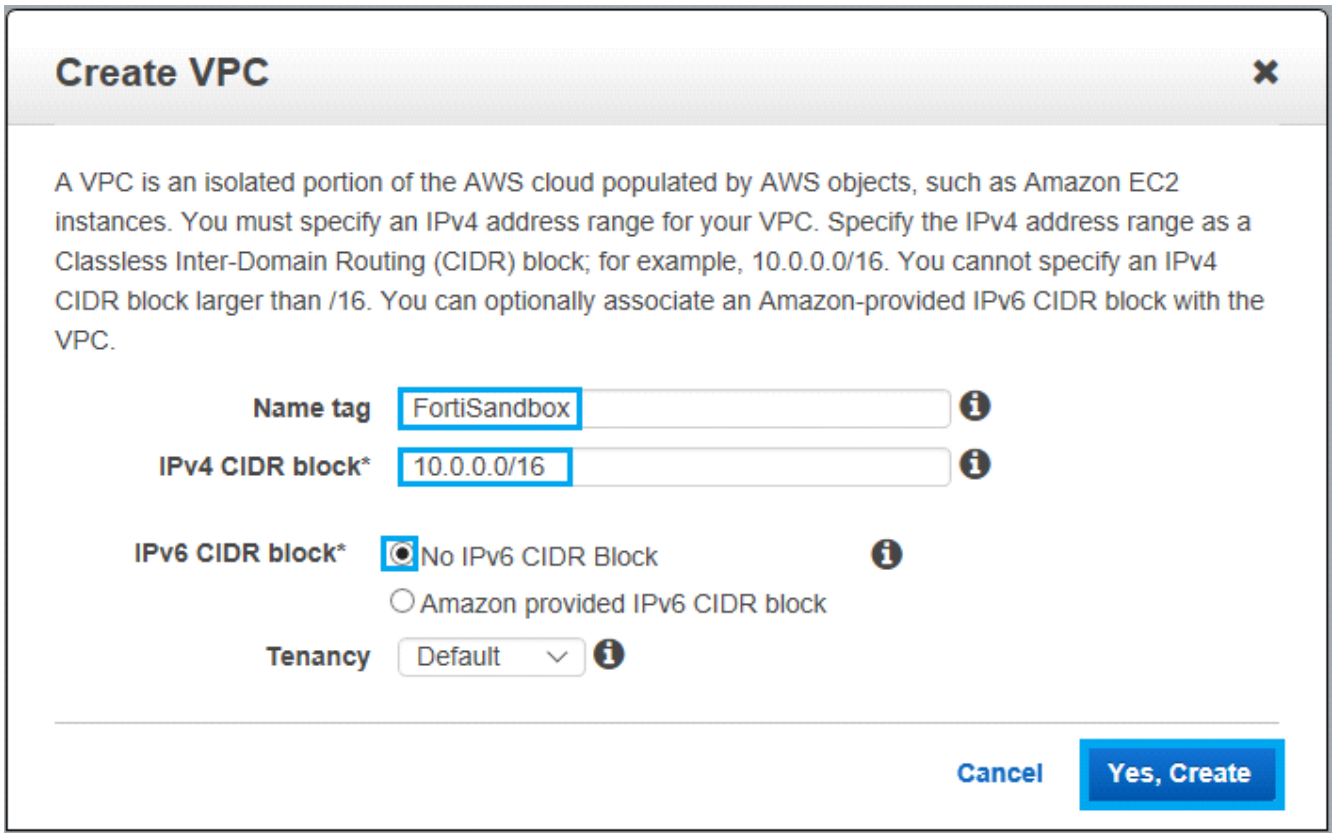
Step 1: Create a Virtual Private Cloud (VPC)

1. Navigate to *VPC Dashboard* > *Your VPCs* > *Create VPC*. The Create VPC dialog box will open.



There's a default VPC but you should always create a new VPC.

2. In the *Name Tag* field, enter a name. For example, FortiSandbox.
3. In the *IPv4 CIDR* field, enter *10.0.0.0/16*. This will ease scale-out issues in the future.
4. In the *IPv6 CIDR Block* field, select *No*.
5. In the *Tenancy* field, select *Default* from the dropdown list.
6. Click *Yes, Create* to create the new VPC.



Step 1.2: Create the Subnet for FortiSandbox Firmware

You will need to create two subnets for FortiSandbox.

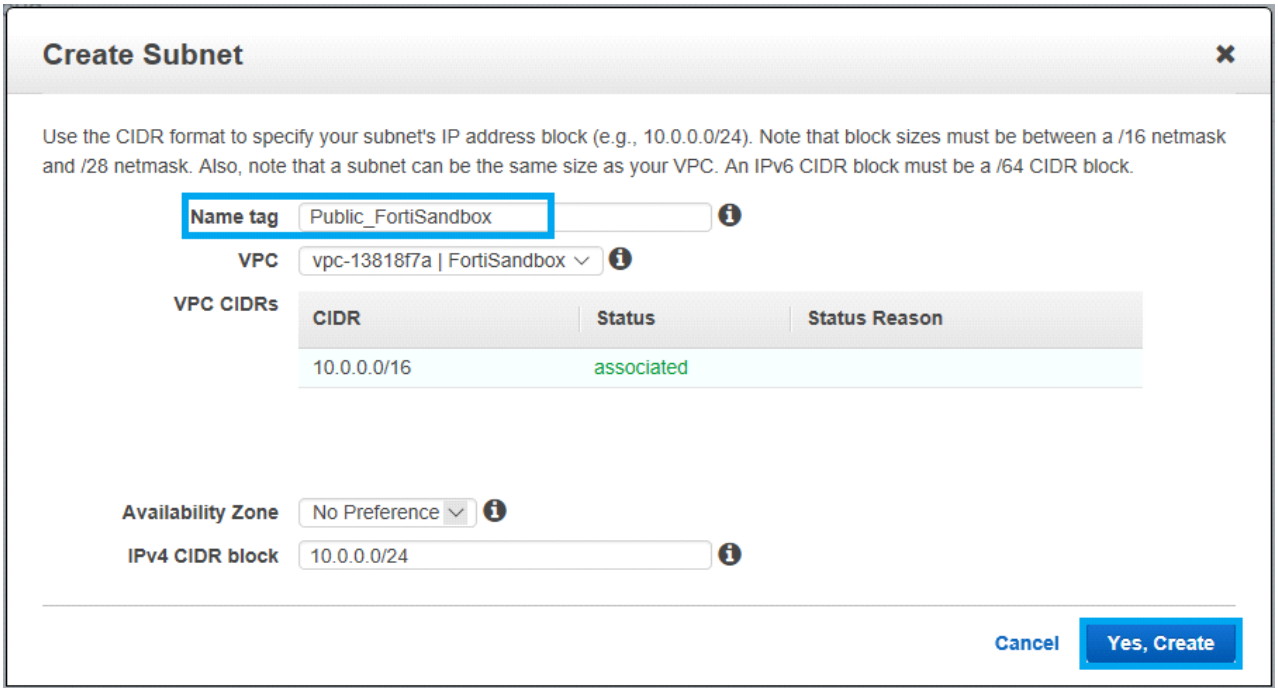
- Public subnet with IPv4 CIDR 10.0.0.0/24, which is connected to the FSA-VM management interface.
- Private subnet with IPv4 CIDR 10.0.1.0/24, which is connected to all VM clones and FSA-VM.

You can skip creating Private subnet if you do not use Trial VMs or Custom VMs. Without a Private subnet, you can still use the Remote VM for file analysis.

To create the Public Subnet:

1. Click *Subnets* > *Create Subnet*. The Create Subnet dialog box will open.
2. In the *Name Tag* field, enter a name. For example, `Public_FortiSandbox`.
3. In the *VPC* field, select the VPC you have just created.
4. In the *IPV4 CIDR block* field, enter *10.0.0.0/24* (public subnet).

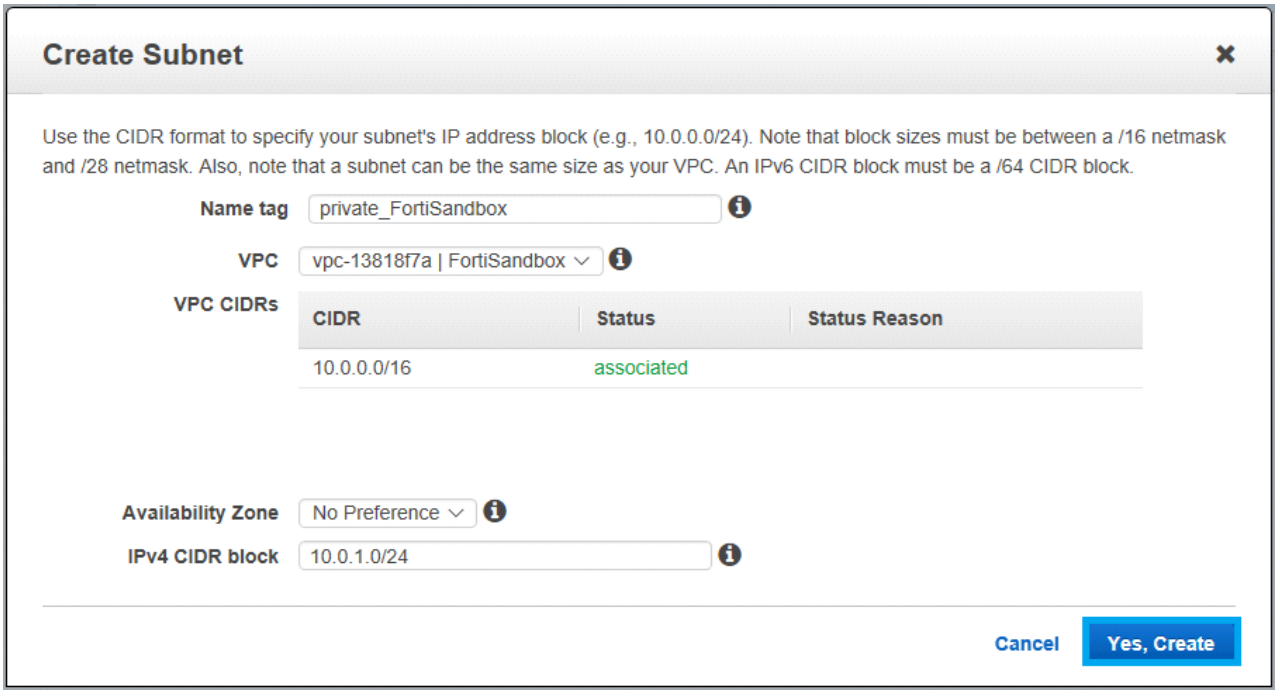
5. Click *Yes, Create* to create the new subnet.



To create the Private Subnet:

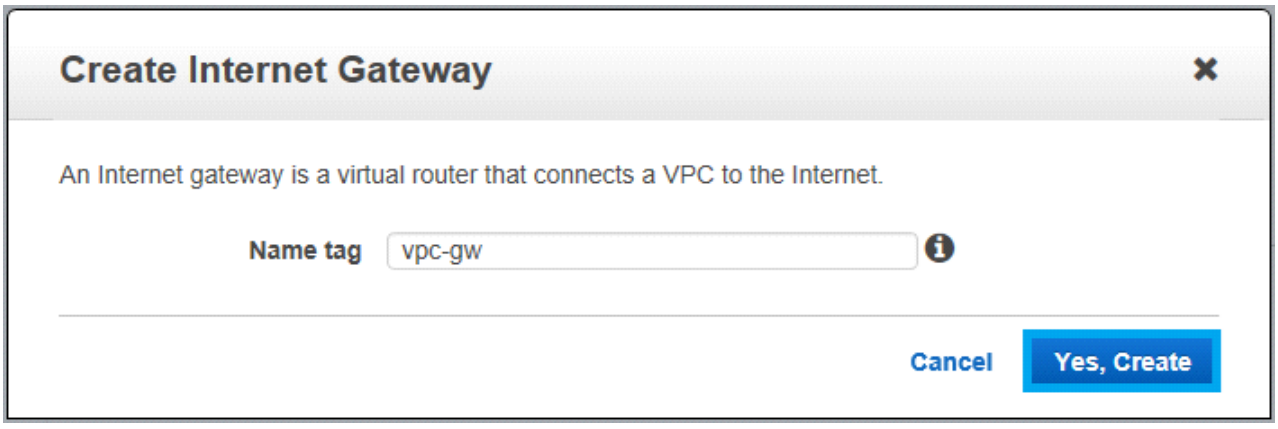
1. Click *Subnets* > *Create Subnet*. The Create Subnet dialog box will open.
2. In the *Name Tag* field, enter a name. For example, Private_FortiSandbox.
3. In the *VPC* field, select the VPC you have just created.
4. In the *IPV4 CIDR block* field, enter *10.0.1.0/24* (private subnet).

5. Click *Yes, Create* to create the new subnet.



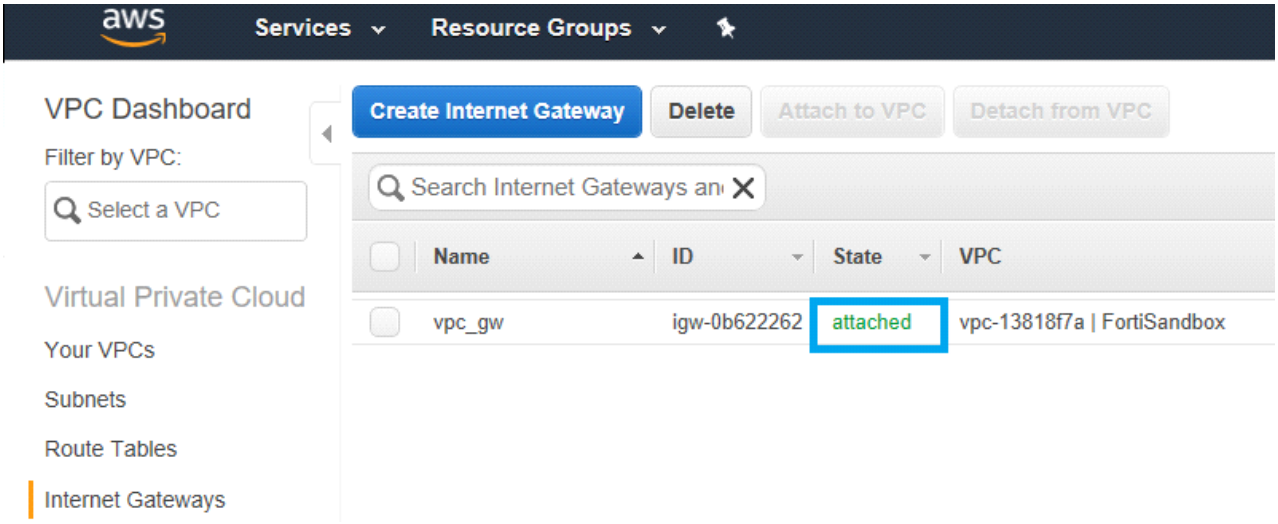
Step 1.3: Create the Internet Gateway

1. Under *Virtual Private Cloud*, select *Internet Gateways*.
2. Click *Create Internet Gateway*.
3. In the *Name Tag* field, enter a name. For example, *vpc-gw*.
4. Click *Yes, Create*.



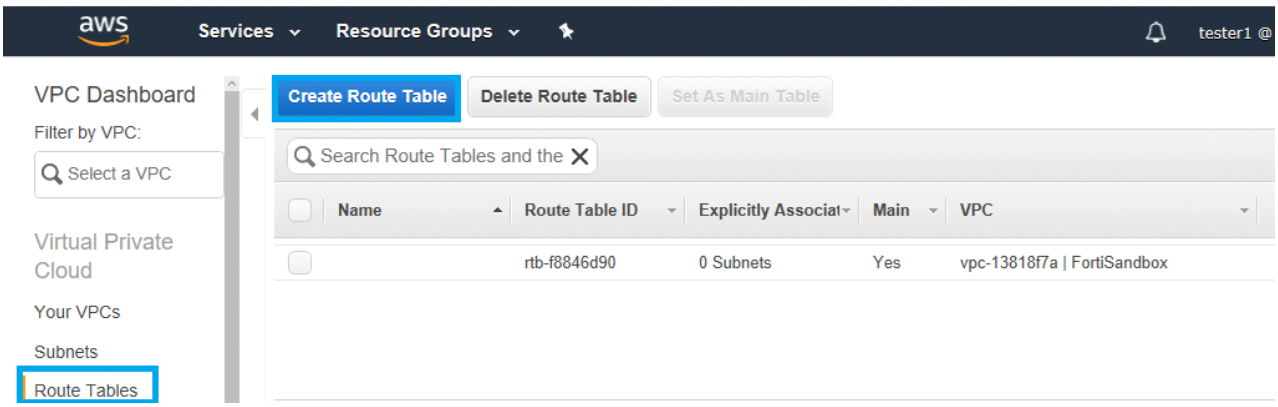
5. Once the Internet Gateway is created, click *Attach to VPC*.

6. Select your created VPC, and click *Yes, Attach*.

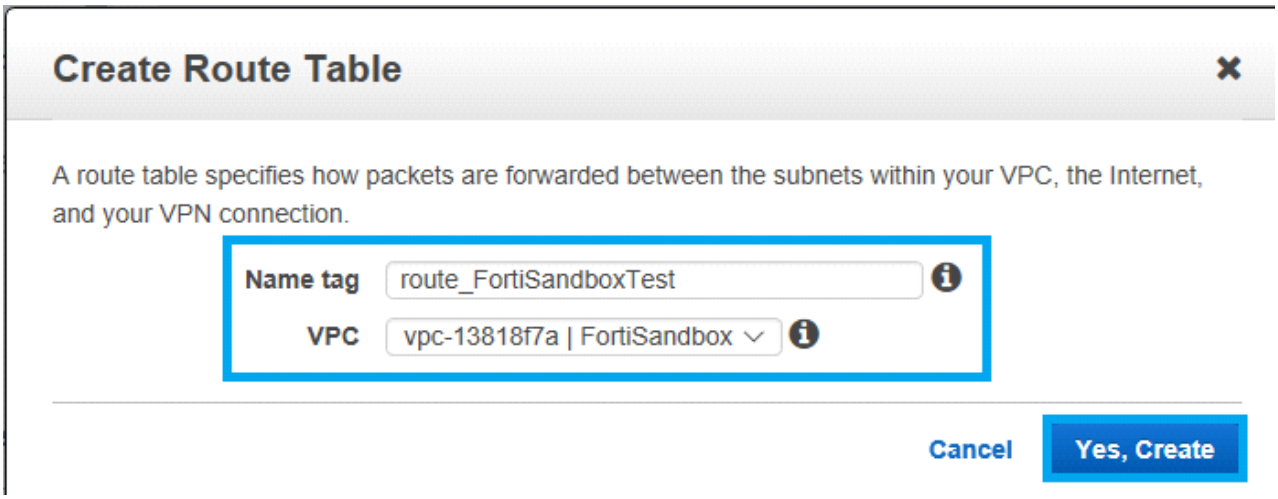


Step 1.4: Create Route Table

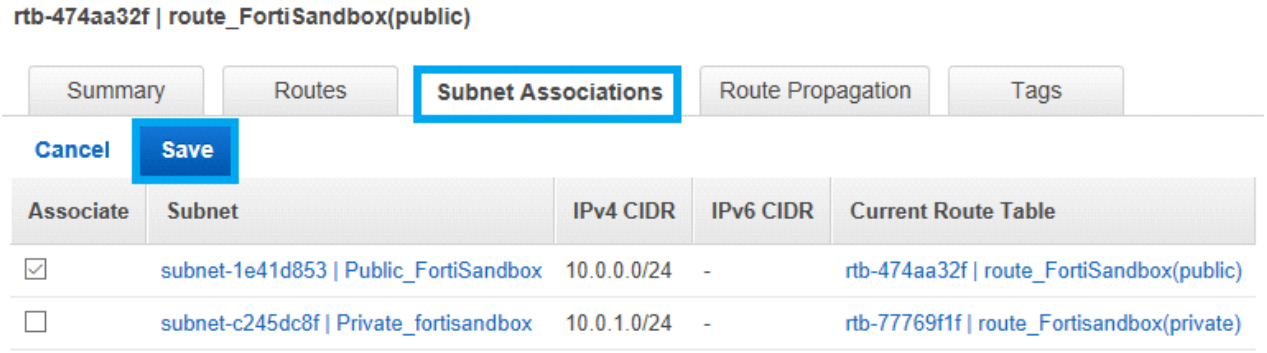
1. Under *Virtual Private Cloud* > *Route Tables* > *click Create Route Table*. The *Create Route Table* dialog box will open.



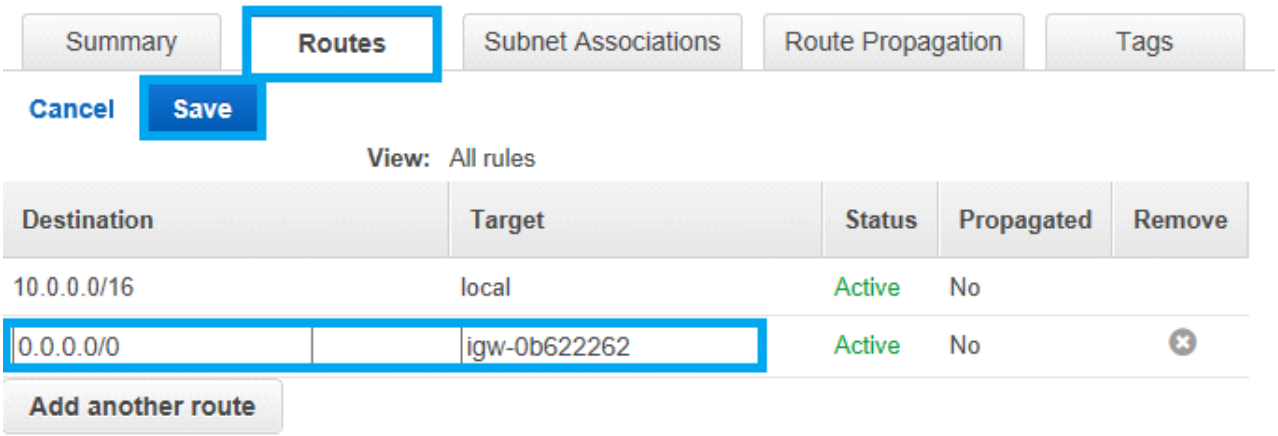
2. In the *Name Tag* field, enter a name. For example, `route_FortiSandboxTest`.
3. In the *VPC* field, select the VPC you created.
4. Click *Yes, Create*.



5. Go to *Subnet Associations* > *Edit* and select the public subnet you created. Click *Save*.



6. Go to *Routes* > *Add Another Route*.
7. In the *Destination* field, enter `0.0.0.0/0`.
8. In the *Target* field, select the internet gateway for the public subnet. Click *Save*.

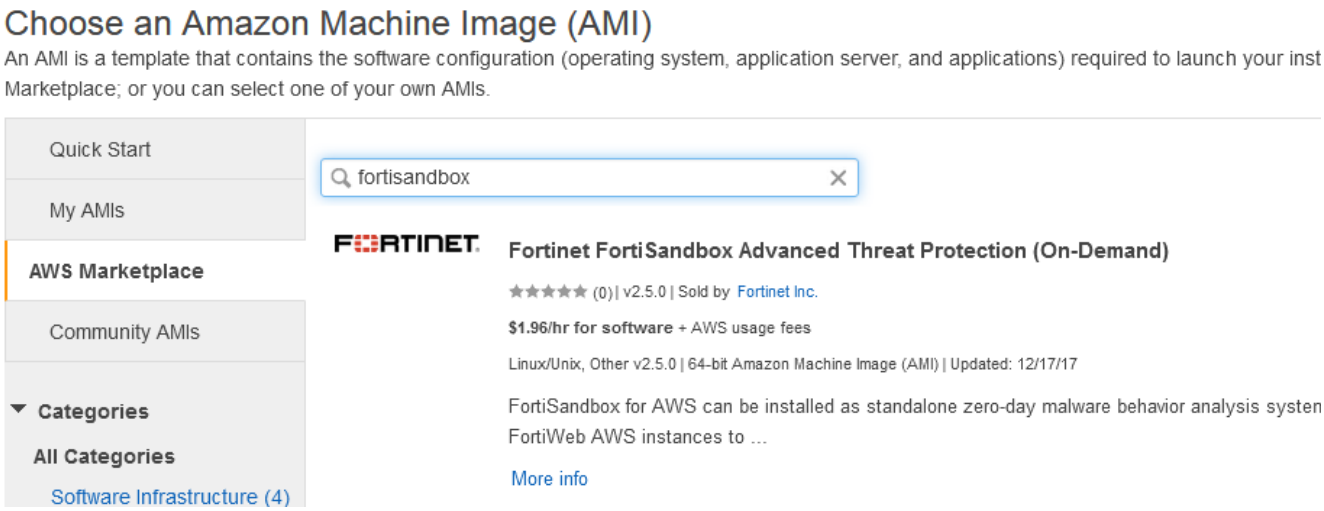


FortiSandbox Provisioning

Step 2: EC2 Launch FSA Virtual Instance

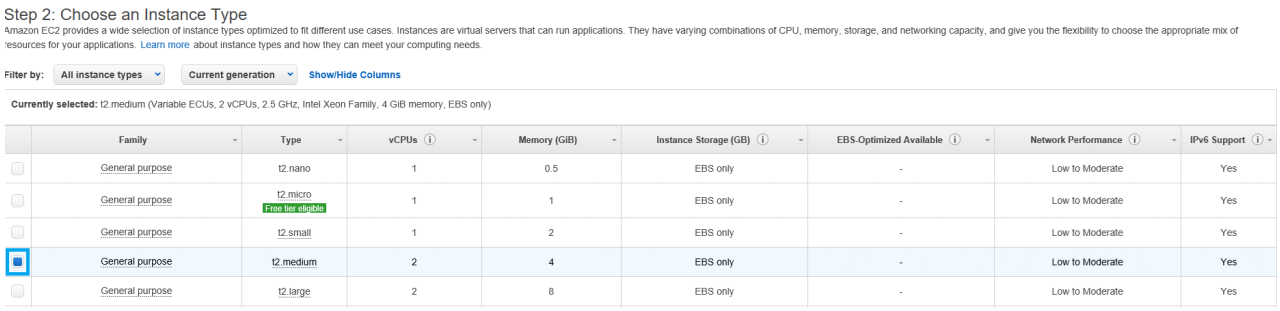
Step 2.1: Amazon Image Machine

In the FortiSandbox search on AWS Marketplace, choose a FortiSandbox Amazon Machine Image.



Step 2.2: Choose an Instance Type

1. From the list, select *t2.medium* for balanced burstable performance
2. Click *Next: Configure Instance*.



Step 2.3: Configure Instance

Configure the following instance details:

Details	Values
Number of Instances	1
Purchasing Option	N/A
Network	Select the FortiSandbox VPC you created
Subnet	Select the public subnet your created
Auto-Assign Public IP	Disable
IAM Role:	None
Shutdown Behavior	Stop
Enable Termination Protection	N/A
Monitoring	N/A
Tenancy	Shared - Run a shared hardware instance
eth0	Select the public subnet you created; Auto-Assign (or any IP in that subnet)
eth1	Select the private subnet you created; Auto-Assign (or any IP in that subnet)

You can skip adding **`eth1`** if you do not use Trial VMs or Custom VMs. You can always add it back when the instance has *Stopped*.

Step 2.4: Add Storage

After configuring the Instance Details, click *Next, Add Storage*.

Step 2.5: Add Tags

Do not configure anything on this page. Click *Next, Configure Security Group*.

Step 2.6: Configure Security

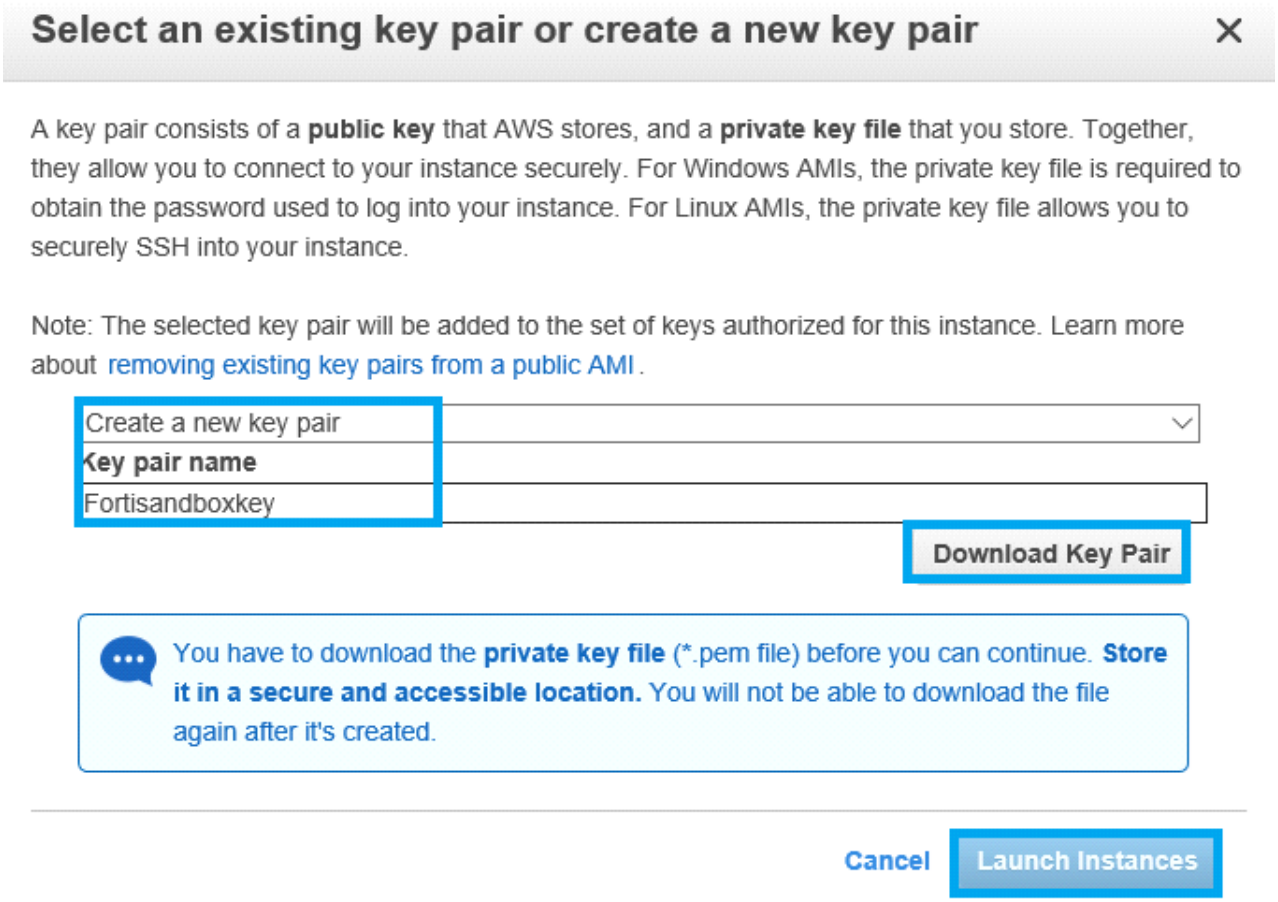
1. Click *Create a New Security Group*.
2. Enter a name for the security group.
3. Provide a description for the security group.
4. Configure the following:

Detail	Value
Type	All Traffic
Protocol	All
Port Range	This value will be automatically selected when you select *All* under Protocol
Source	Custom. Enter `0.0.0.0/0` as the SourceIP

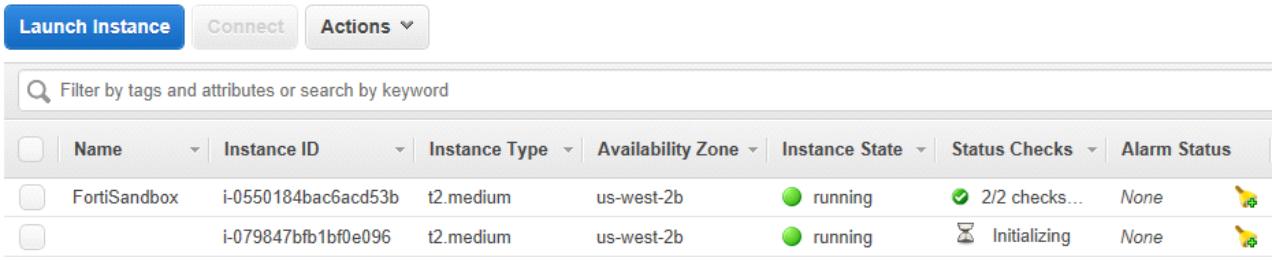
5. Click *Review and Launch*.

Step 2.7: Review Instance Launch

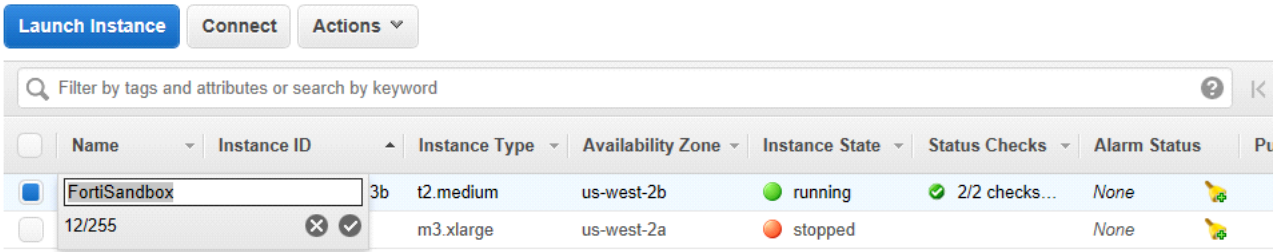
1. Review the page for the correct instance details.
2. Click *Launch*. A dialog box will open to *Create a New Key Pair*.
3. Enter a *Key Pair Name*.
4. Click *Download Key Pair* and save the private key file.
   You can import an existing public key for remote access to the running instance.



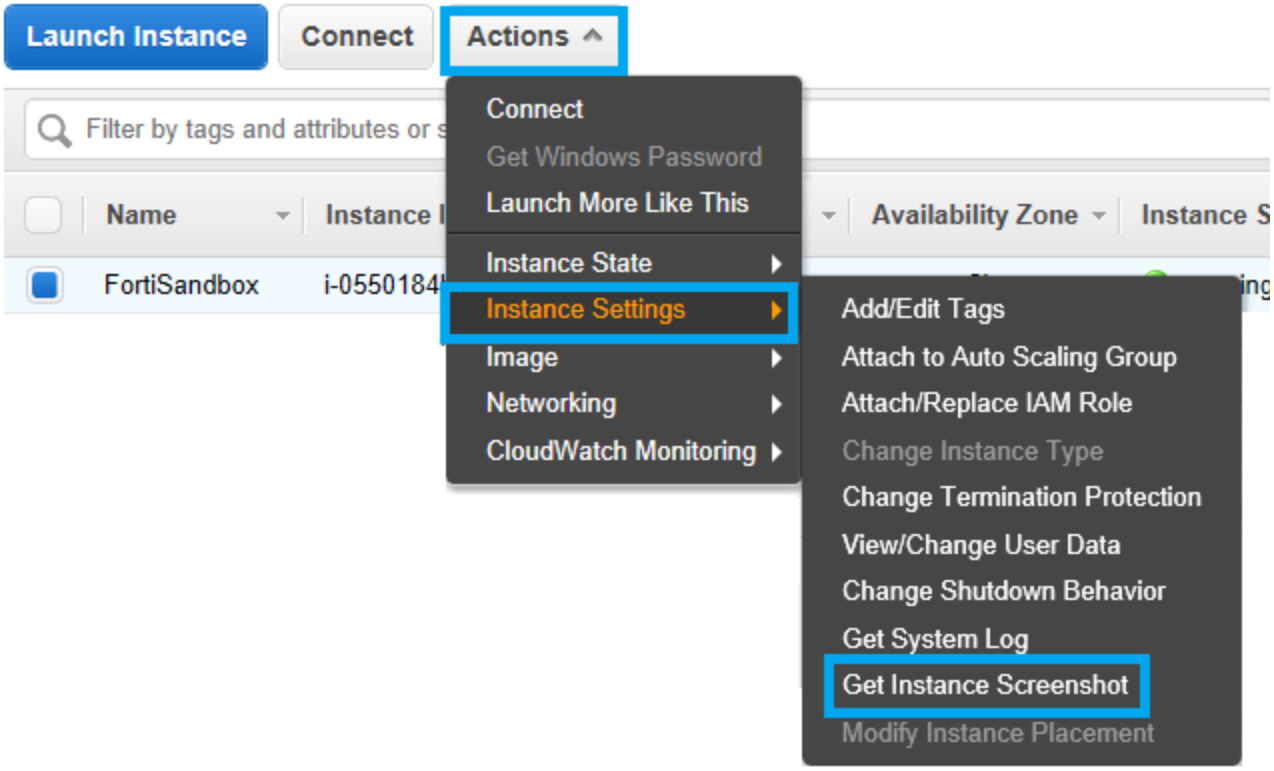
5. Click *Launch Instances*.
   After launching the instance, the next page displays the FortiSandbox instance up and running
6. Click *View Instances* to view the instance state.
   It will take a few moments for the status to change from *Initializing* to *2/2 Checks*.



7. Once the instance is running, click the instance and enter a name. For example, *FortiSandbox*.



8. Select the created instance then go to *Actions* > *Instance Settings* > *Get Instance Screenshot* to view the status of the launched instance.



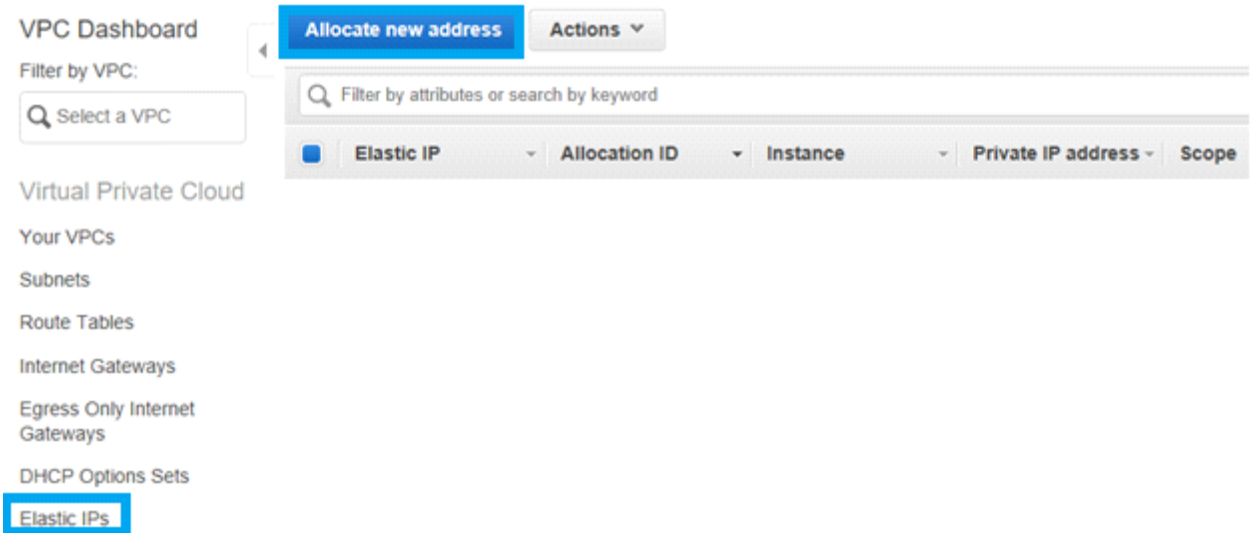
Network Configuration

Step 3: Configure FortiSandbox Network Settings

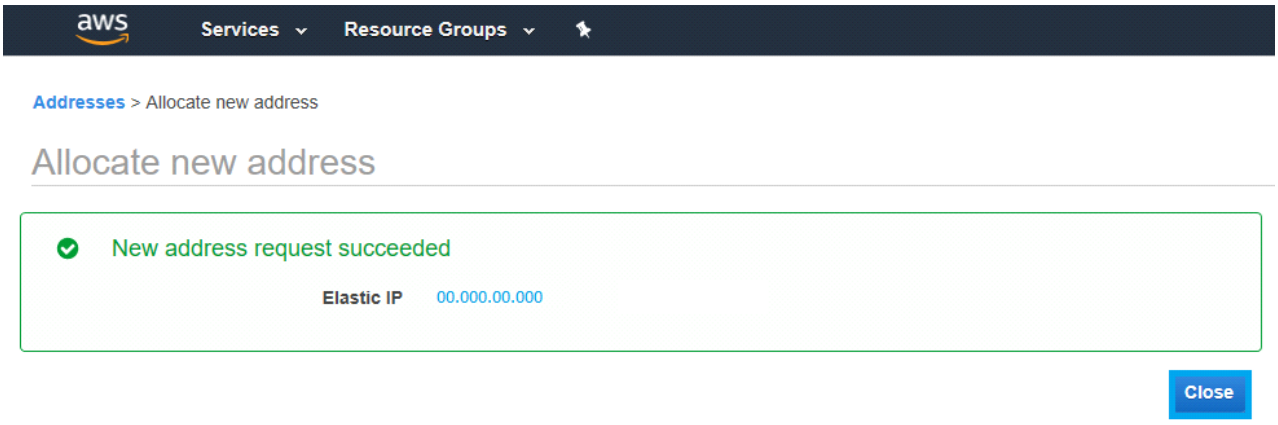
Step 3.1: Assigning Elastic IP to Instance

Create a new Elastic IP (EIP) if there is not already one to allocate under the Virtual Private Cloud.

1. Click *Elastic IPs* > *Allocate New Address*.

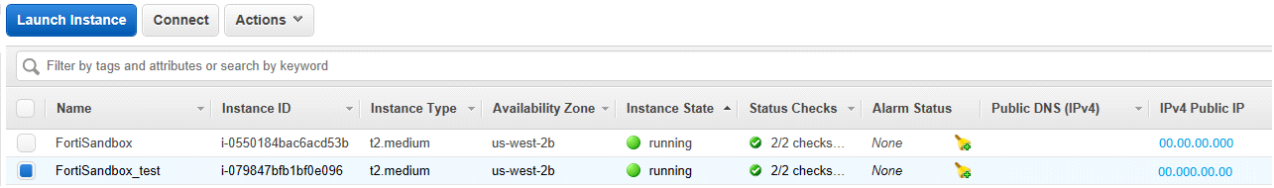


2. Click *Allocate* to get the new EIP Address.
3. Once you see the new *Elastic IP Address*, click *Close*.



Step 3.2: FortiSandbox Web GUI Access

1. Copy the IPv4 Public IP from the created instance.



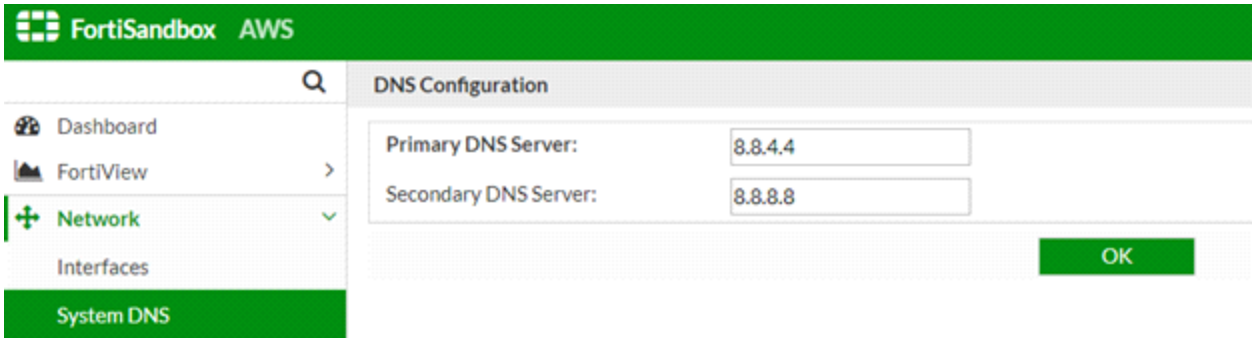
2. Paste the copied IP address into a new browser window to log into the FortiSandbox Web GUI. The default username is admin. The default password is your created Instance ID. You can find this in the EC2 Management Console.

Step 3.3: DNS Configuration

1. Go to *Network* > *System DNS*.
2. Configure the following:

Detail	Value
Primary DNS Server	8.8.4.4
Secondary DNS Server	8.8.8.8

3. Click *OK*.



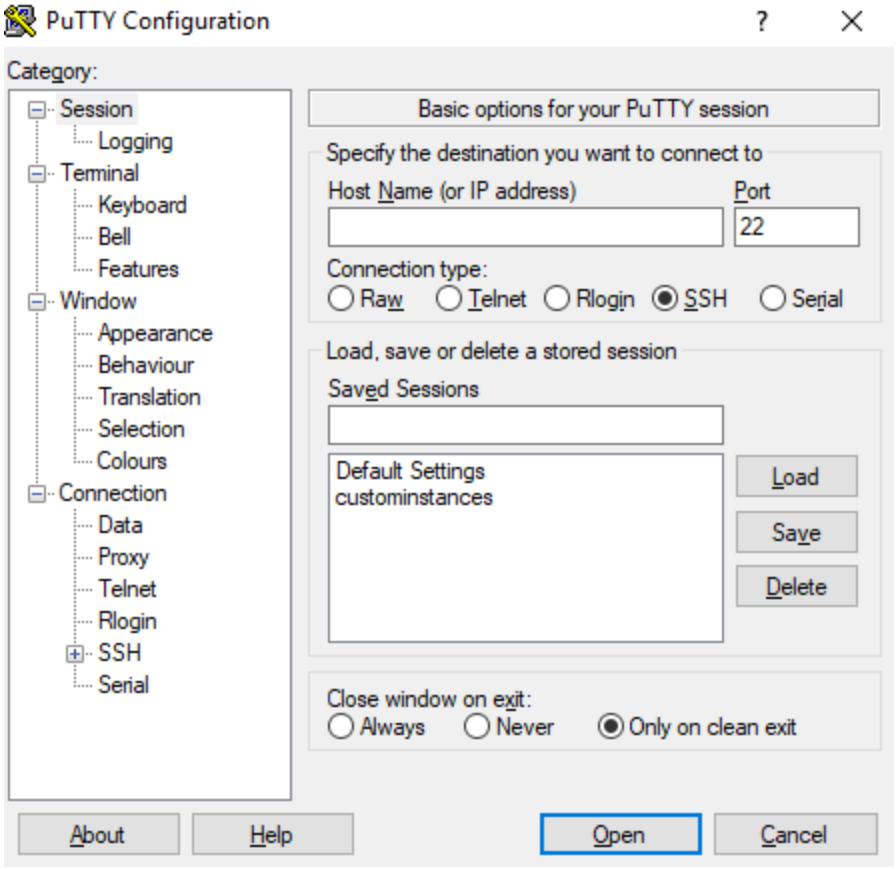
Access FortiSandbox CLI

FortiSandbox has CLI commands that are accessed when accessing the FortiSandbox via console or by using a SSH or TELNET client.

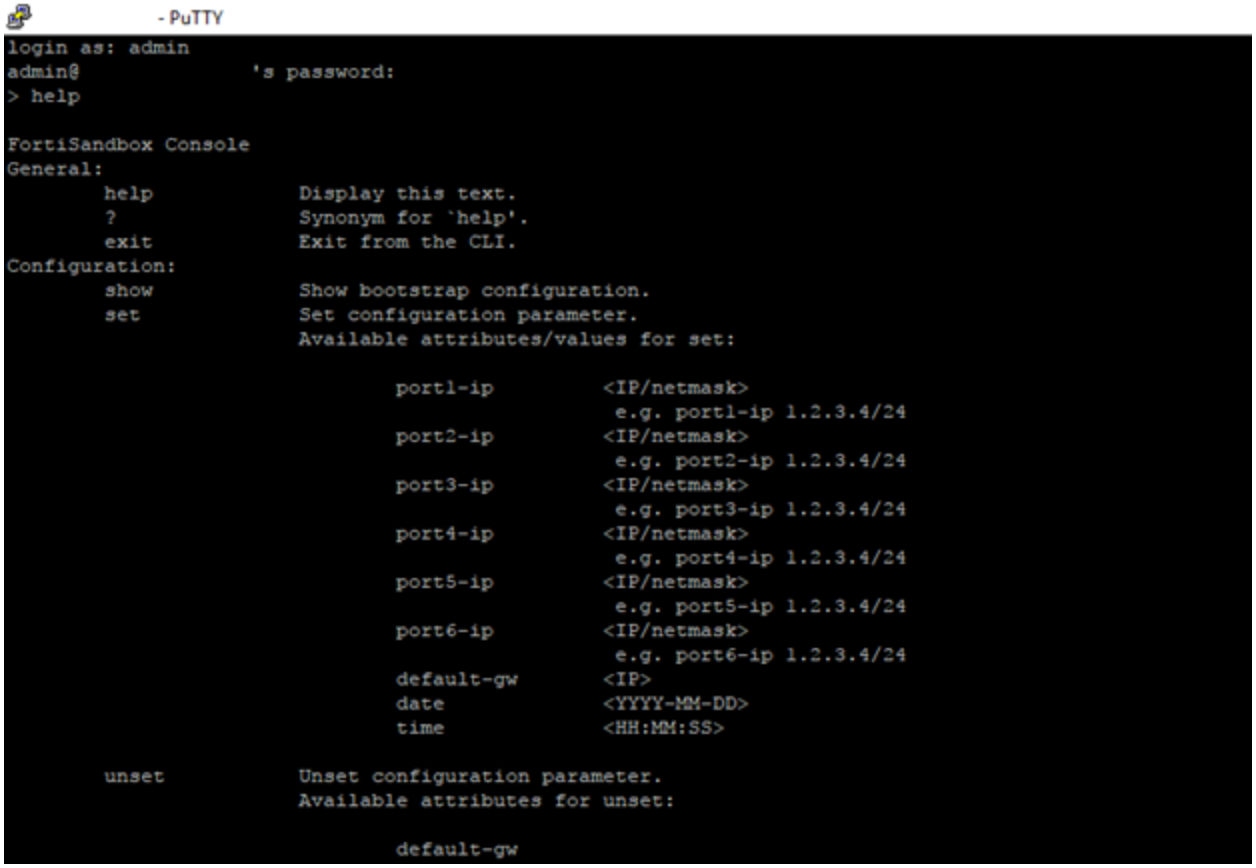
Log into the CLI using the Elastic IP of your created instance by giving the username as admin with the `ppk` file.

If you do not choose the *Without Key Pair* option, log in using password `<InstanceID>`.

Before logging in, convert the saved `pem` file which you downloaded while creating the key pair `ppk` file.



Run the following commands to interact with FortiSandbox using CLI.

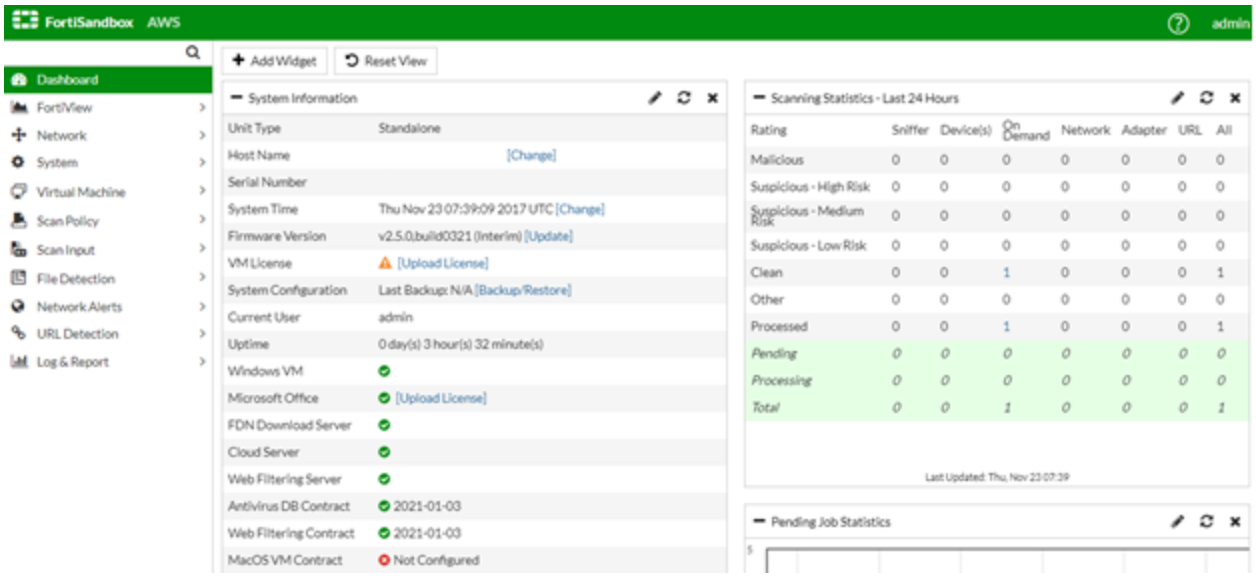


The commands are only for illustration purposes only, you can use relevant commands as per the requirement.

FortiSandbox Testing

Delete this text and replace it with your own content.

Step 4.1 FortiSandbox Dashboard and Contract Information

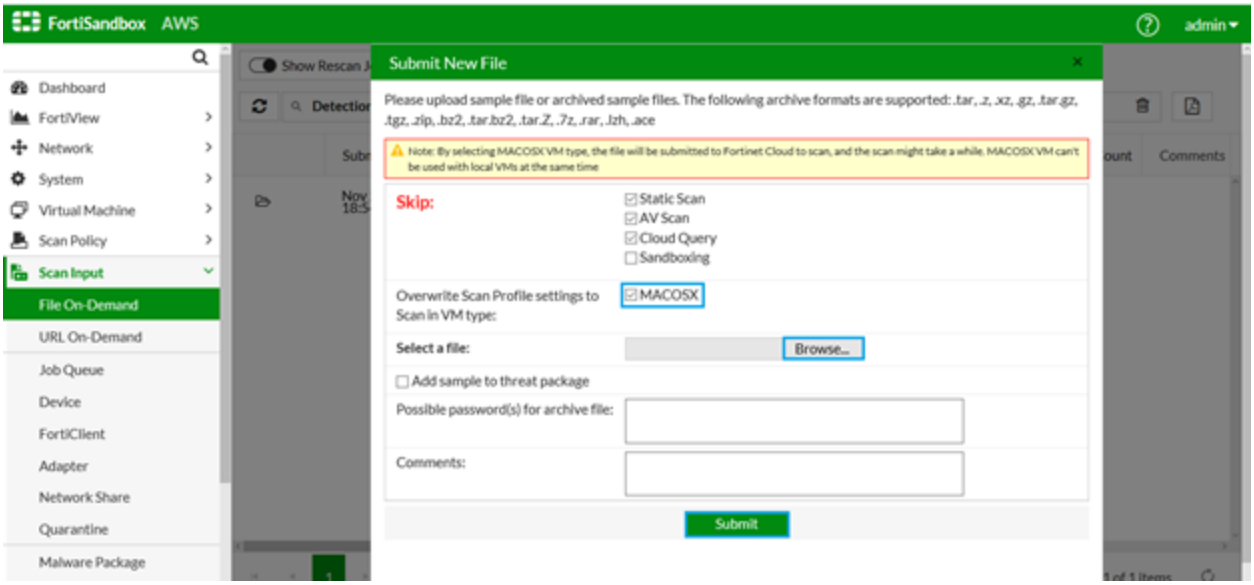


VM License is not needed for AWS FortiSandbox.

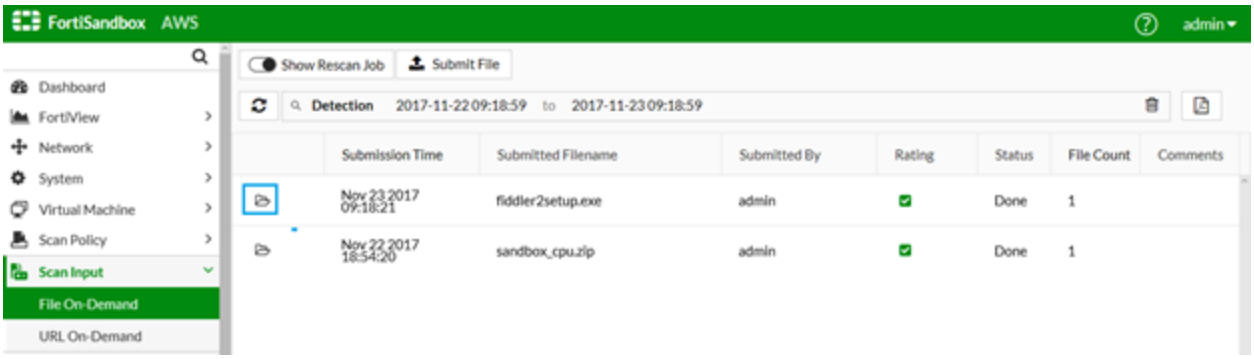
To get future firmware updates, contact Fortinet support site http://support.fortinet.com.

Step 4.2: On-Demand Submit Test using Remote VM

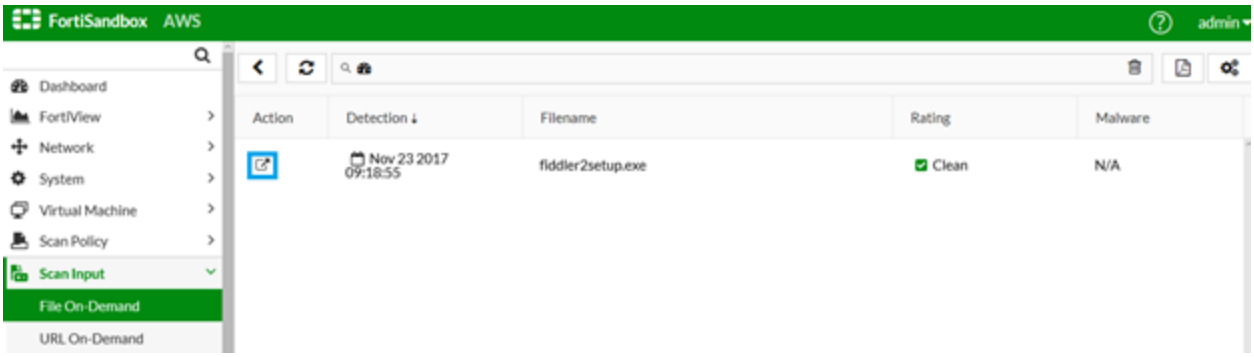
1. Go to *Scan Input* > *File On-Demand* > *Submit File*. The *Submit File* dialog box will open.
2. Click on *Choose File* and upload the `fiddler2setup.exe` file.
3. Click *Submit*. You should receive a `Clean` rating after you send the file to FortiSandbox if the uploaded file is clean not malicious or suspicious.
4. Click *Browse* and upload any file and click *Submit*.



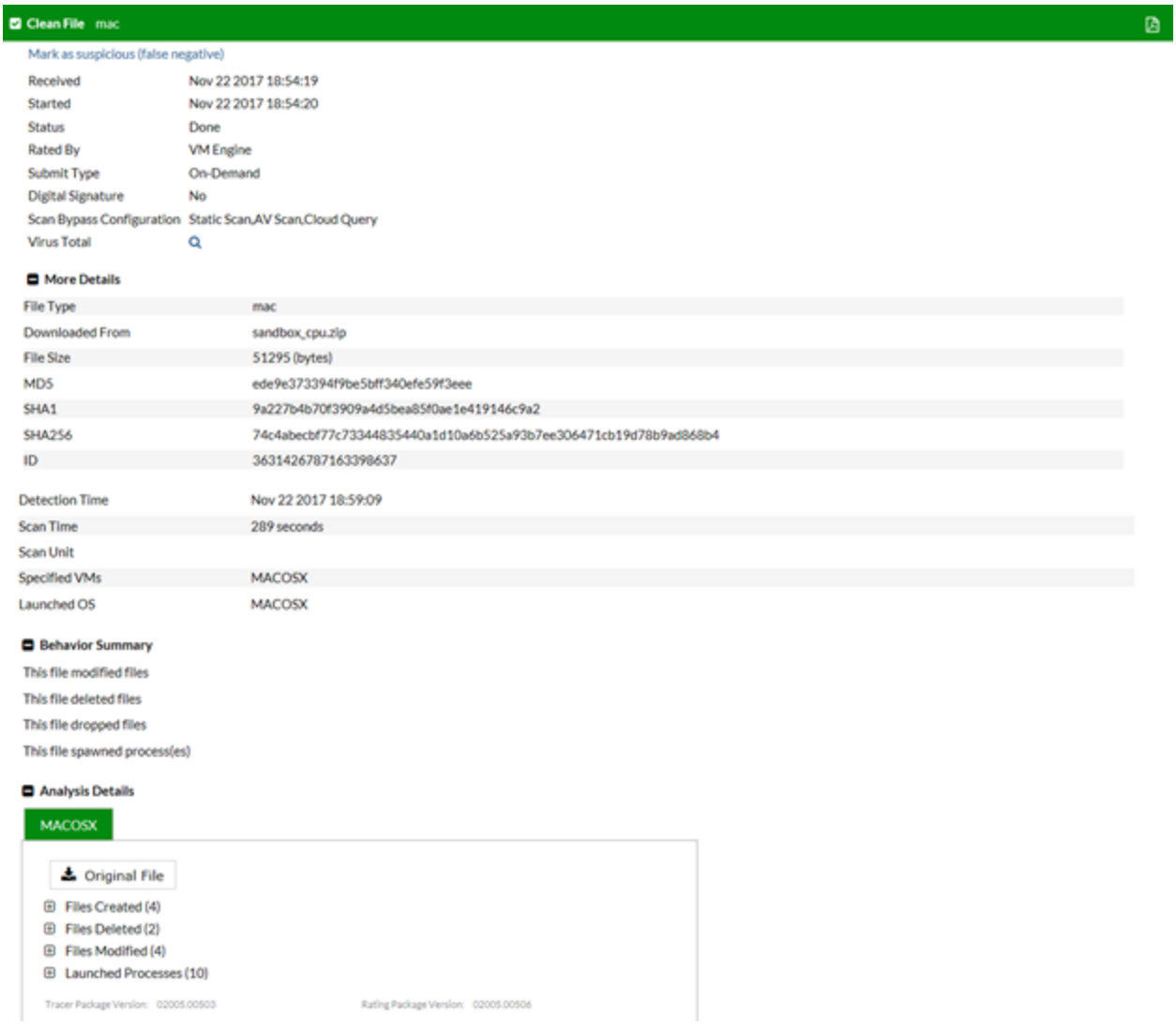
5. After uploading the file, you can view *File On-Demand* and select any file to check.



6. Click the *View File* icon under the Action column.



7. View the file details.


Clean File mac
Mark as suspicious (false negative)
Received Nov 22 2017 18:54:19
Started Nov 22 2017 18:54:20
Status Done
Rated By VM Engine
Submit Type On-Demand
Digital Signature No
Scan Bypass Configuration Static Scan,AV Scan,Cloud Query
Virus Total
More Details
File Type mac
Downloaded From sandbox_cpu.zip
File Size 51295 (bytes)
MD5 ede9e373394f9be5bff340efe59f3eee
SHA1 9a227b4b70f3909a4d5bea85f0ae1e419146c9a2
SHA256 74c4abecbf77c73344835440a1d10a6b525a93b7ee306471cb19d78b9ad868b4
ID 3631426787163398637
Detection Time Nov 22 2017 18:59:09
Scan Time 289 seconds
Scan Unit
Specified VMs MACOSX
Launched OS MACOSX
Behavior Summary
This file modified files
This file deleted files
This file dropped files
This file spawned process(es)
Analysis Details
MACOSX
Original File
Files Created (4)
Files Deleted (2)
Files Modified (4)
Launched Processes (10)
Tracer Package Version: 02005.00503
Rating Package Version: 02005.00506

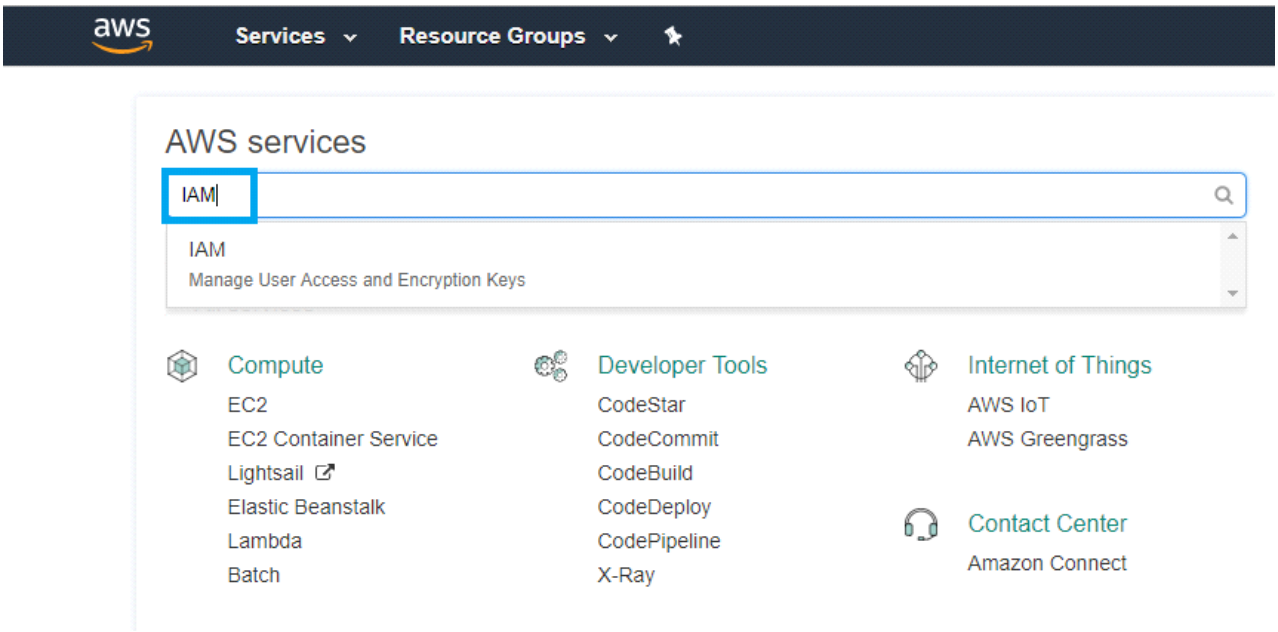
Advanced AWS Setup for using VMs

Step 5: Setup an AWS Account for FortiSandbox

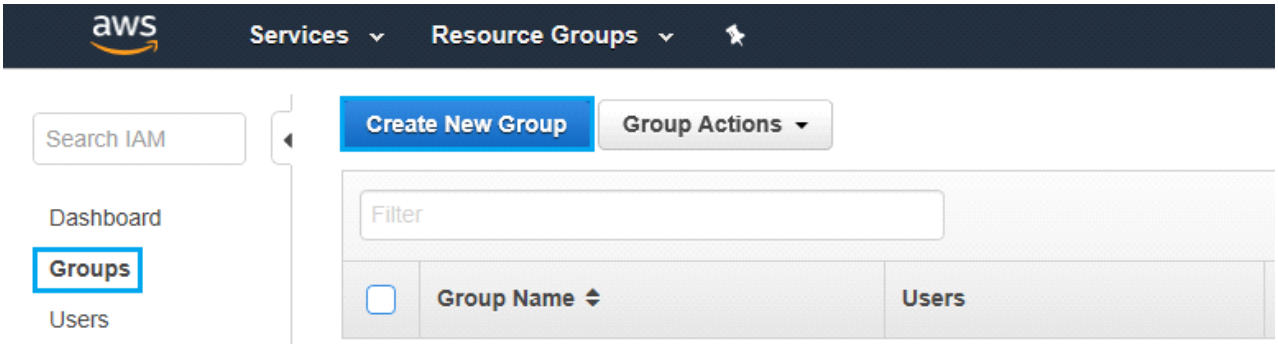
There are a few account preparations required before you launch the FortiSandbox in the AWS Marketplace.

Step 5.1: Create IAM Group and User

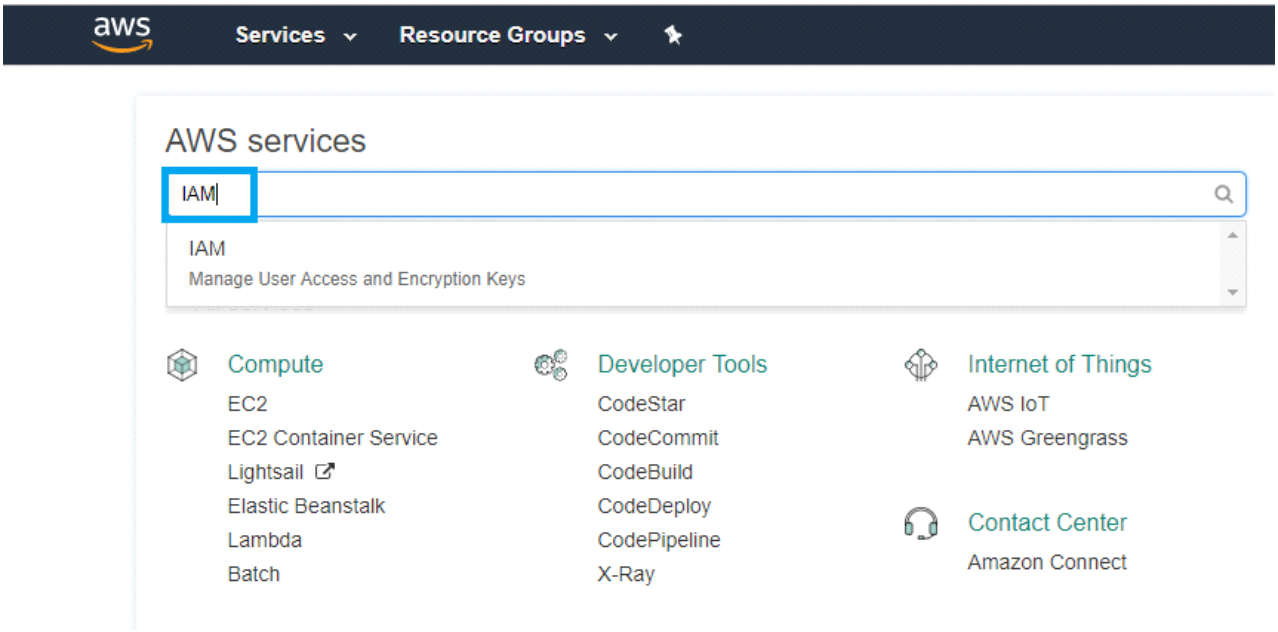
1. You will need to create one or more IAM users from the *AWS Management Console*.
2. Log into the AWS Console with your credentials.
3. Click *Search* and enter *IAM* in the search field.



4. Click *Groups* > *Create New Group*.



5. In the *Group Name* field, enter a name. For example,QA_FortiSandboxTest.

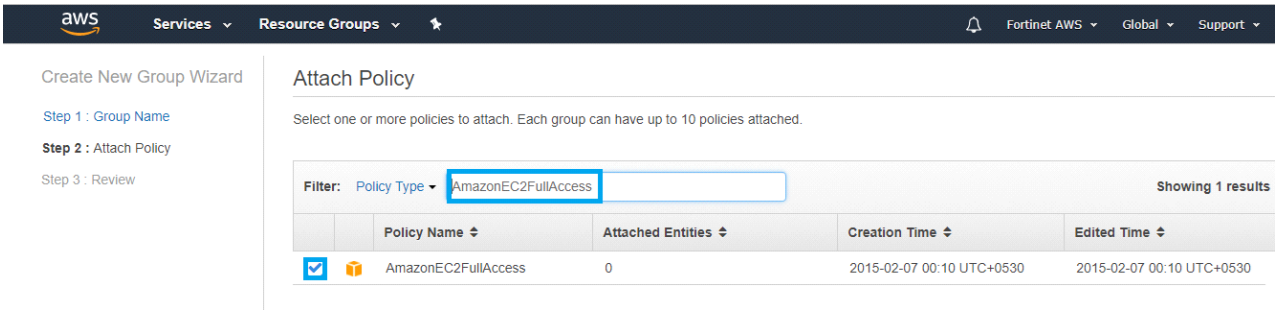


Step 5.2: Attach Policy

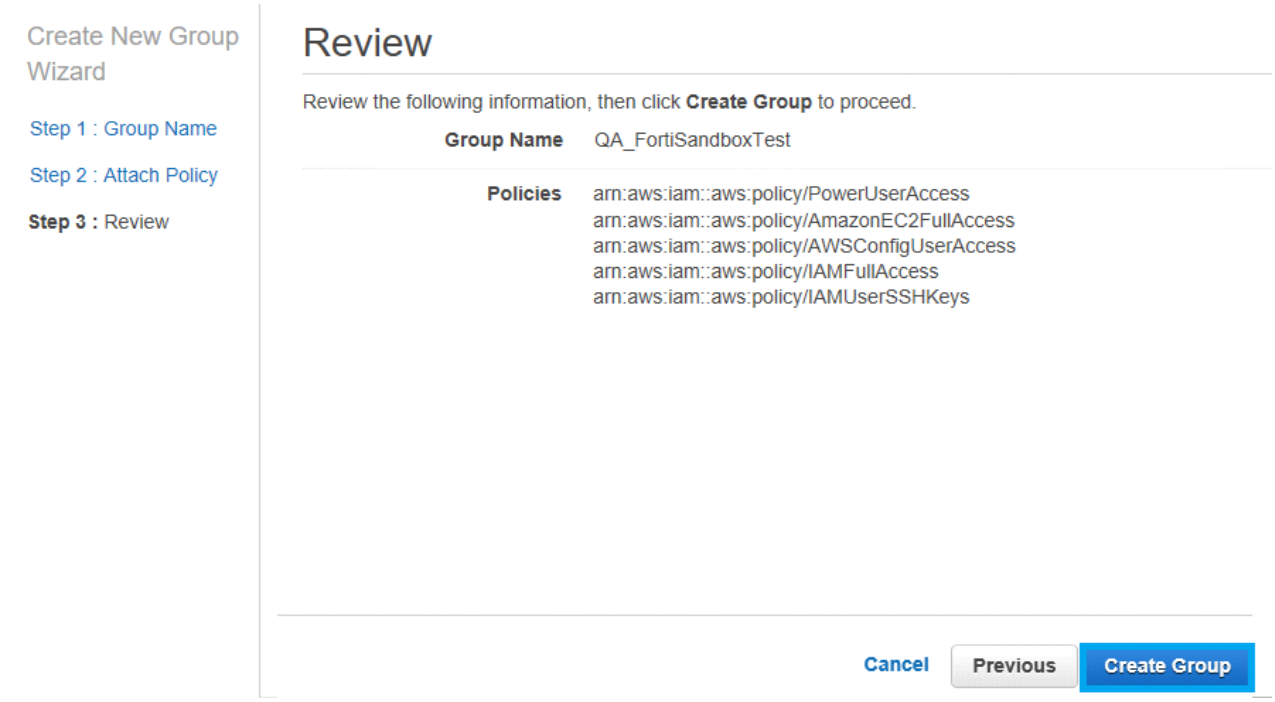
Ensure you have the correct permissions before you attach policies to a group. The following list are the policies that need to be added to the Group previously created (QA_FortiSandbox).

- AmazonEC2FullAccess
- AWSConfigUserAccess
- IAMUserChangePassword
- IAMUserSSHKeys
- PowerUserAccess
- IAMFullAccess

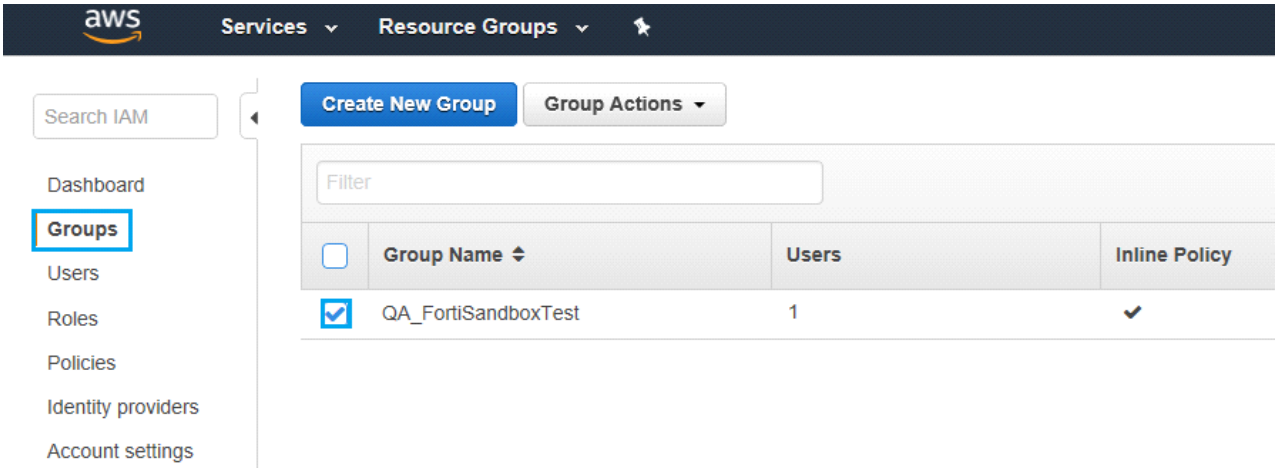
1. Click *Filter* and enter `AmazonEC2FullAccess`
2. Check the check box.



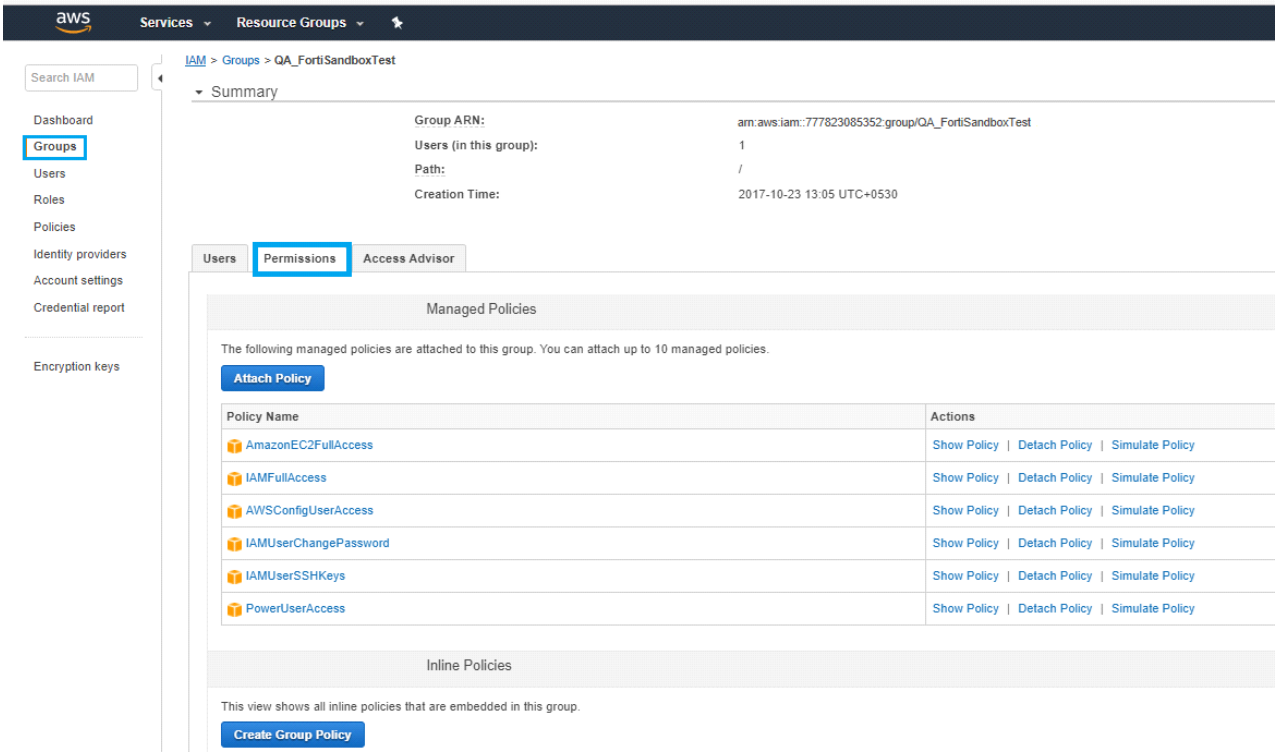
3. Repeat this for all the policies.
4. After reviewing, click *Create Group*. The group should be listed under *Groups*.



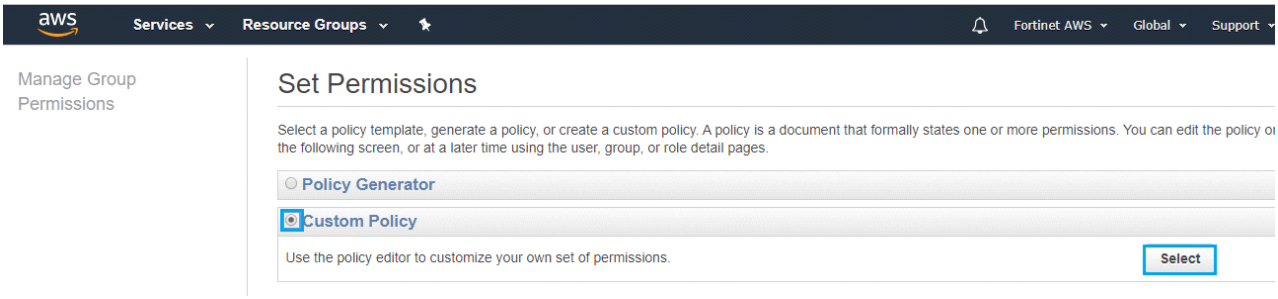
5. Check the group you created (`QA_FortiSandbox`) to review the group summary.



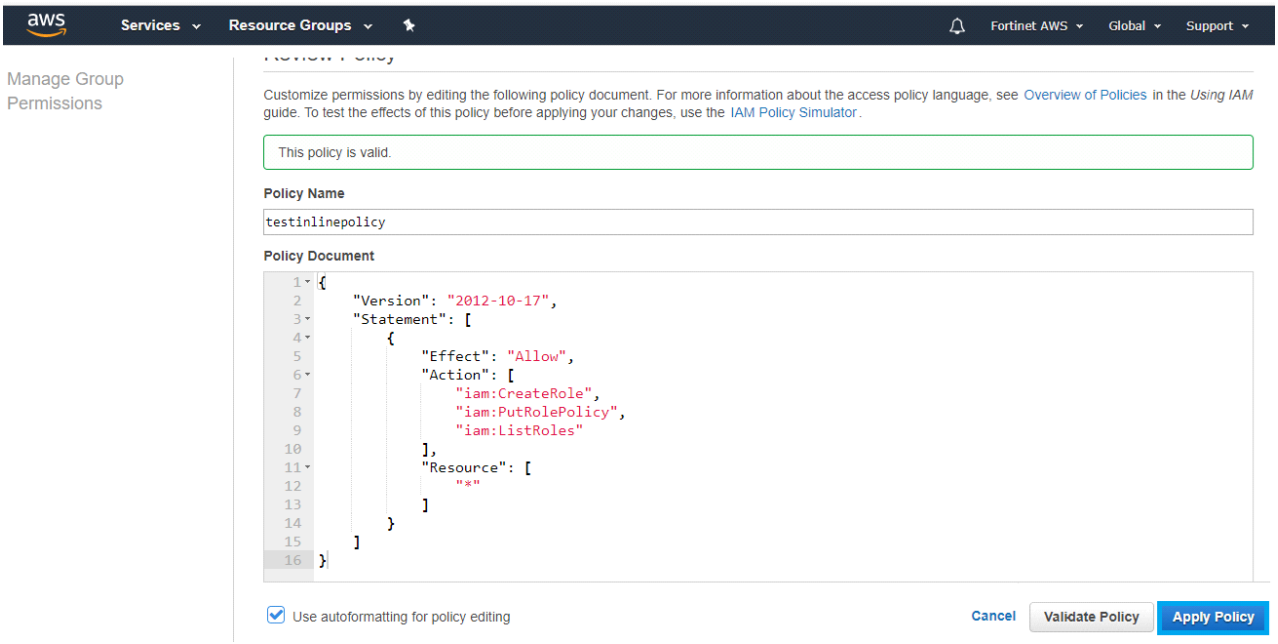
6. Under *Permissions*, review the attached policies.
7. Under *Inline Policies*, click *Create Group Policy*.



8. Select *Custom Policy* and use the policy editor to customize your own set of permissions.



9. Enter a policy name and code.
10. Click *Validate Policy*. If validation is successful, click *Apply Policy*.

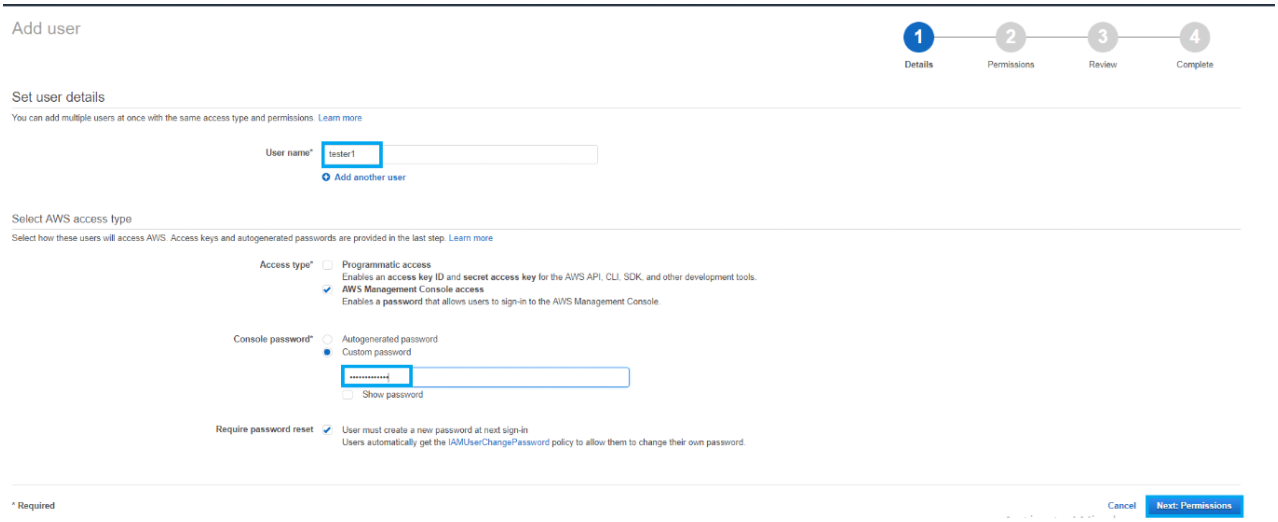


11. Under *Inline Polices*, you can review created policy names.

Step 5.3: Create IAM Users and AWS API Key

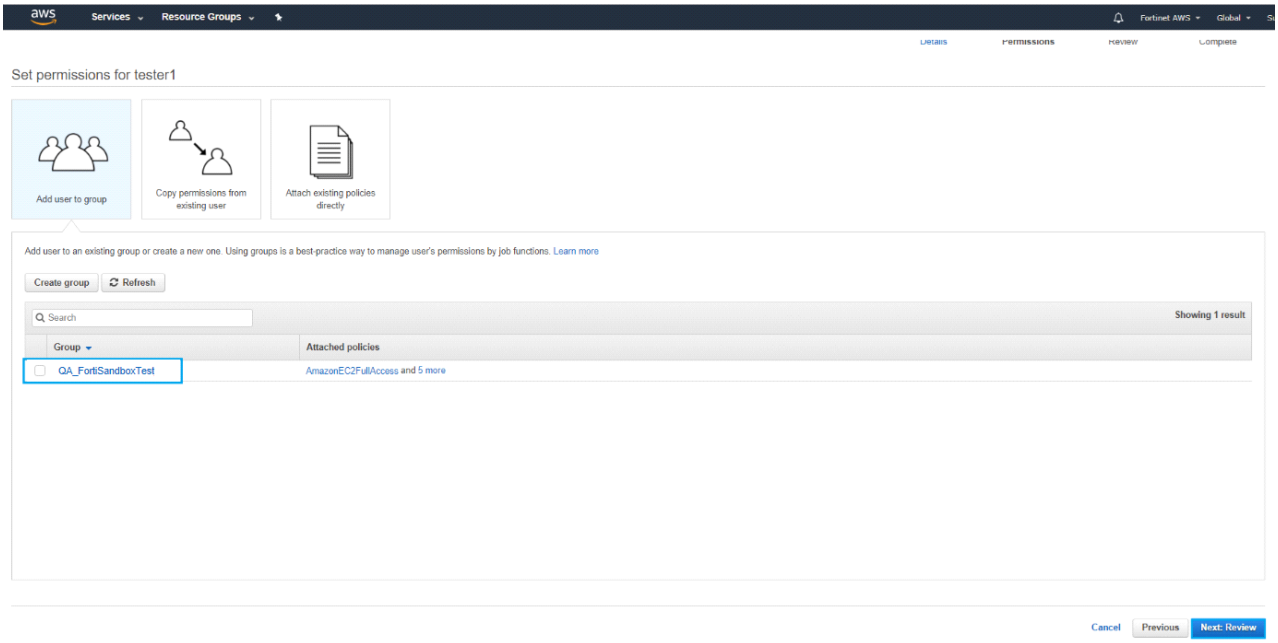
IAM Users

1. Under *Users* > *click Add User*.
2. Provide the username and select AWS Management Console Access.
3. In the *Console Password* field, select *Custom Password*.
4. Click *Next Permissions*.

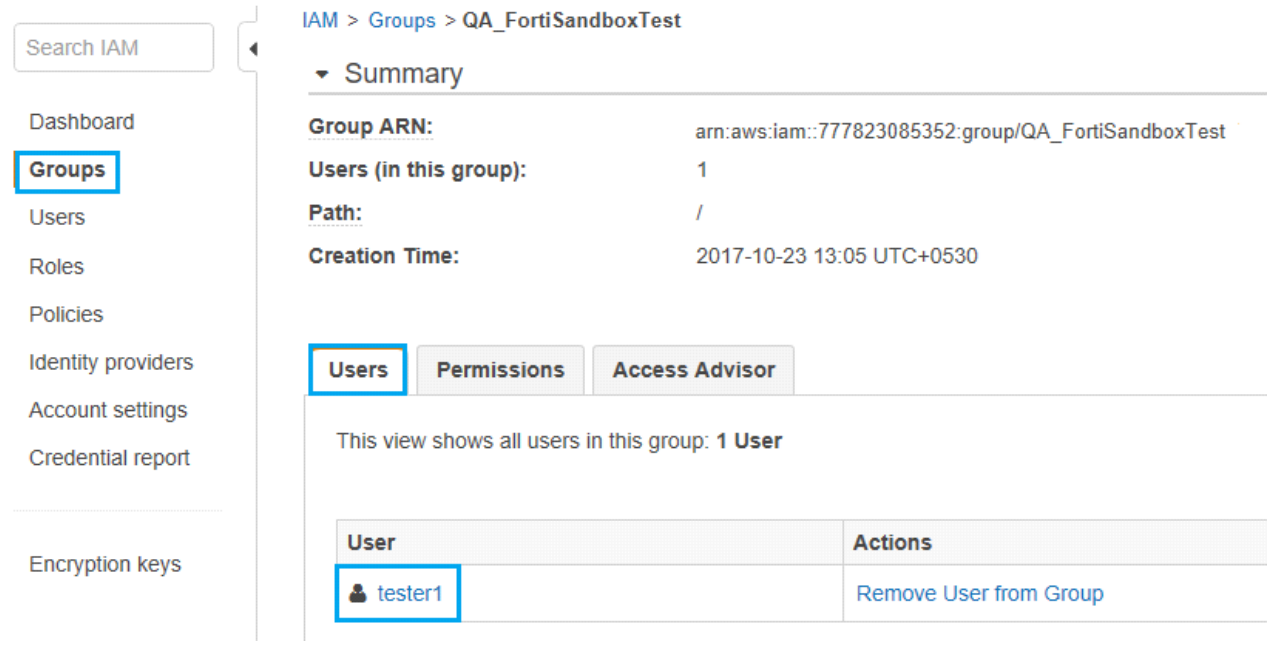


5. Search for the *Group Name* you created (`QA_FortiSandbox`).

6. Click *Next Review*.



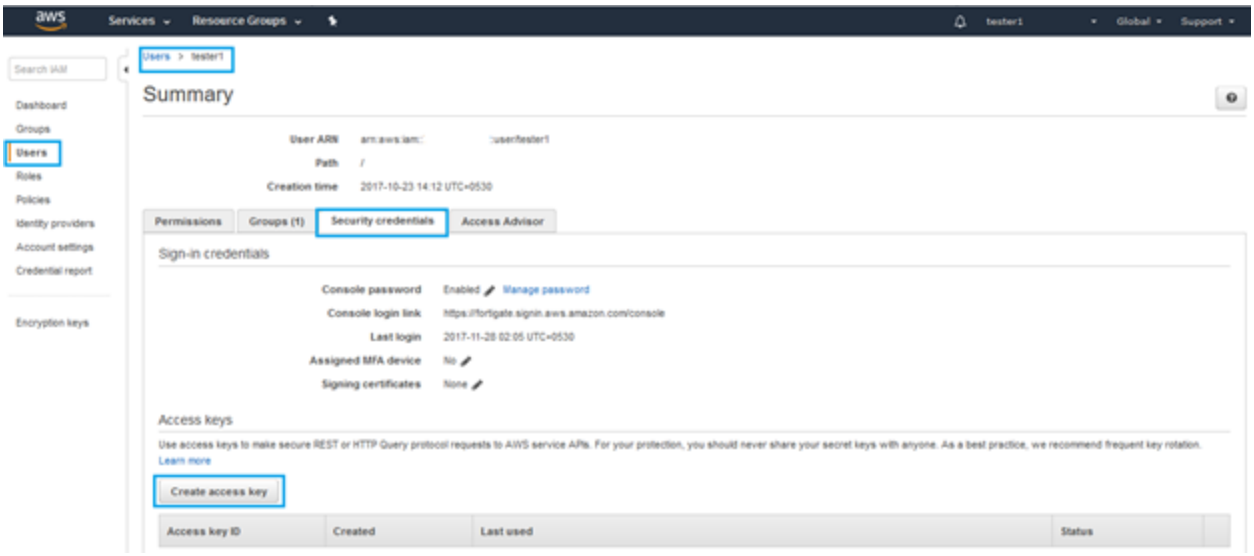
7. Once you have added the group, click *Create User*.
8. Click *Close*.
9. After adding the user to the group, click on *Groups* to view the user.



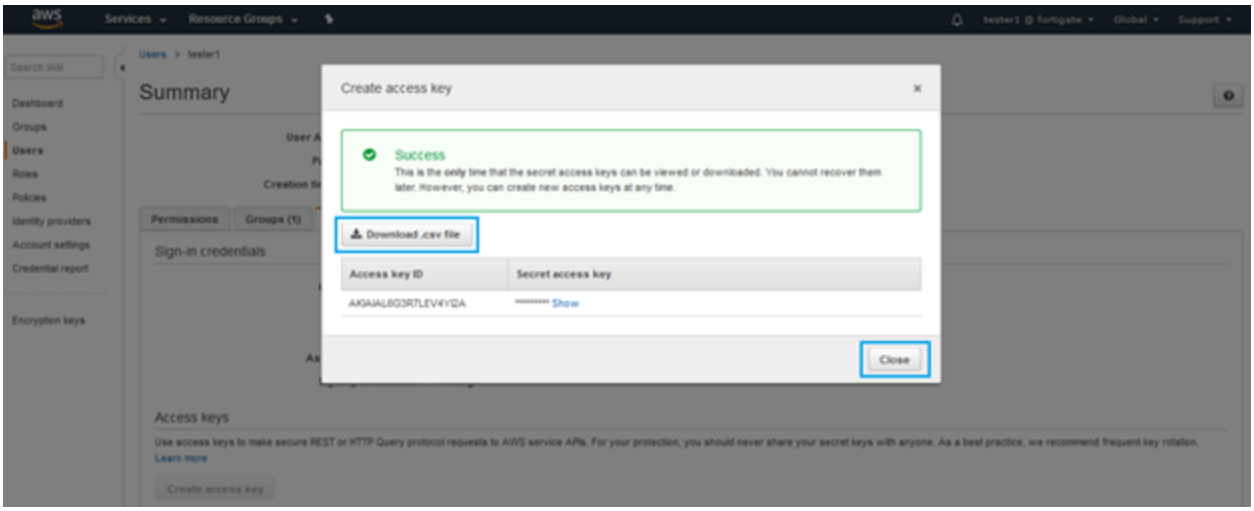
10. Sign out from AWS and sign in with the user you created.
11. Give the user login credentials and reset the password. Click *Confirm* to change the password.

AWS API Key

1. API Gateway supports multiple mechanisms of access control, including metering or tracking API uses by clients using API keys.
2. To create AWS API key, navigate to *IAM> Users > created user > Security Credentials > Create Access Key*. The Create Access Key dialog box will open.



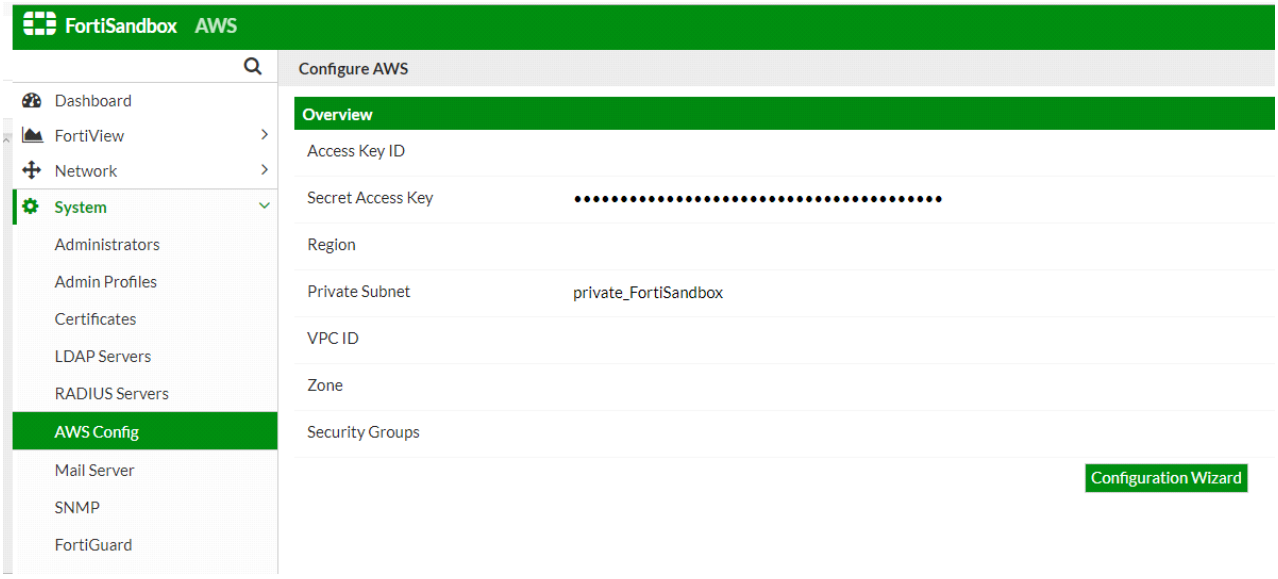
3. Click on *Download.csv file* to save the access key ID and save the access key to a CSV file on your computer.



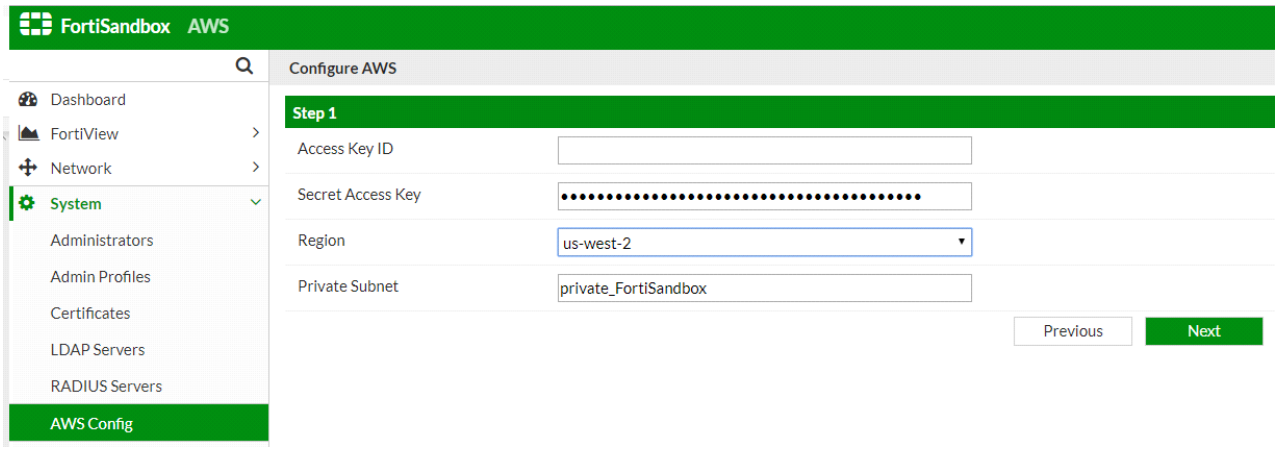
4. Click *Close*.

Step 5.4: FSA GUI AWS Configuration

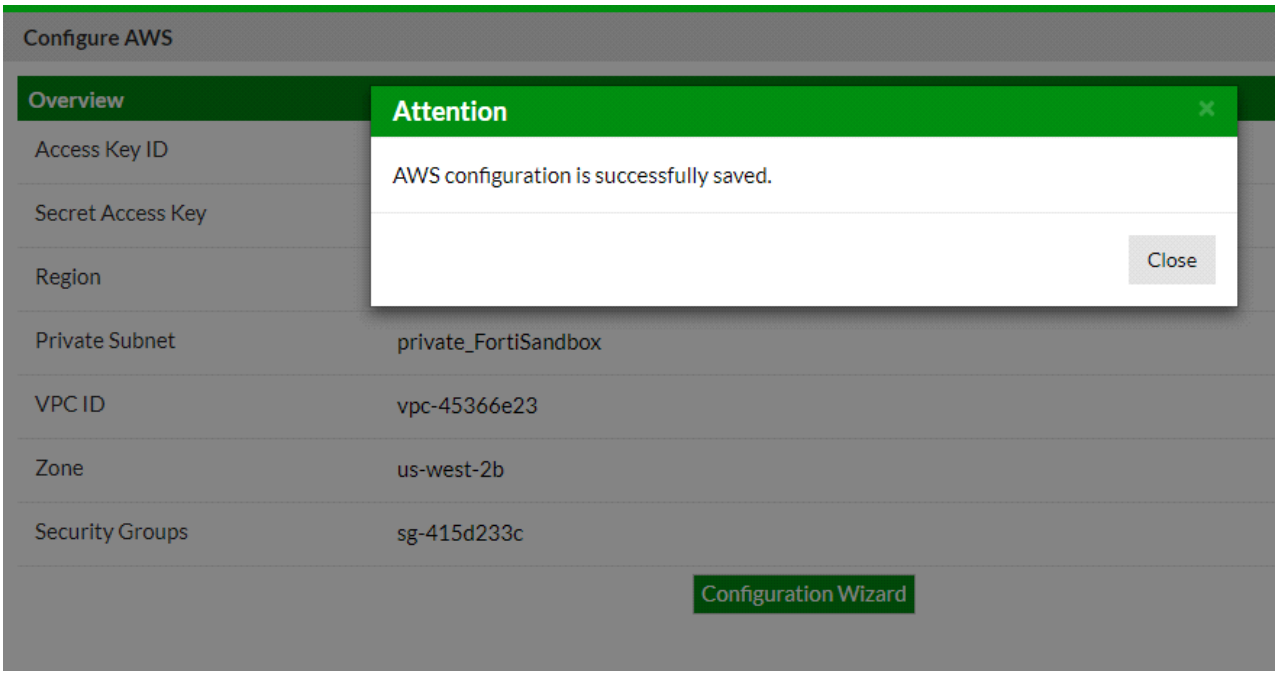
1. Navigate to *System > AWS Config*, and fill in the required AWS API key information with the setup wizard.
2. Enter the *private IP* address name in *Private Subnet* field.
3. Click *Configuration Wizard*.



4. In the *Region* field, select `us-west-2` from the drop down.



5. Click *Next*.
6. Enter the *VPC ID* you created.
7. Click *Next*.
8. Enter the *Security Group ID* you created.
9. Click *Save*.
10. Once AWS configuration is successfully saved, click *Close*.

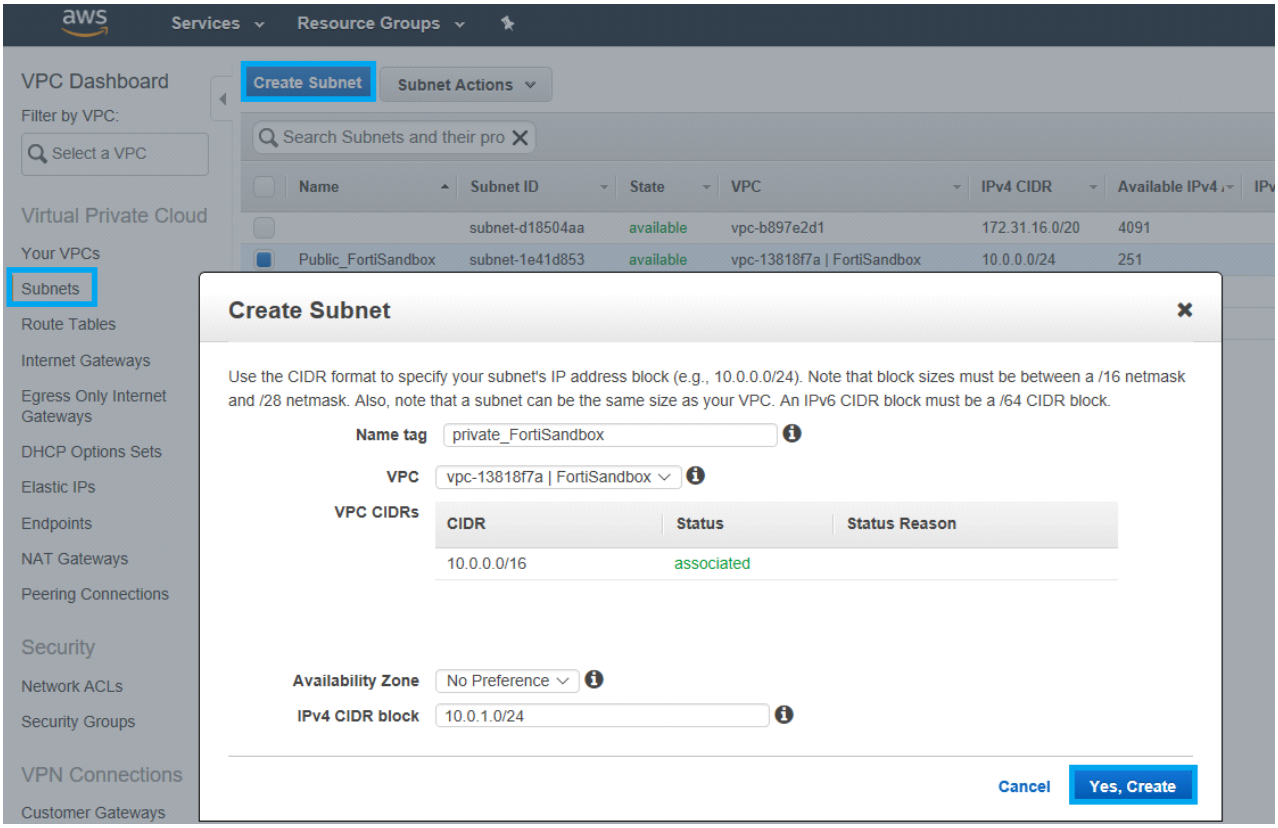

Configure AWS
Overview
Access Key ID
Secret Access Key
Region
Private Subnet
private_FortiSandbox
VPC ID
vpc-45366e23
Zone
us-west-2b
Security Groups
sg-415d233c
Configuration Wizard
Attention
AWS configuration is successfully saved.
Close

Prepare VM Subnet for FortiSandbox

Step 6.1: Create Private Subnet

The Private Subnet (IPv4 CIDR 10.0.1.0/24) is connected to all VM clones and FSA-VM.

1. Click *Create Subnet*. The Create Subnet dialog box will open.



2. Under the *Name Tag* field, enter a name. For example, `private_FortiSandbox`.
3. Under *VPC*, select the VPC you created.
4. In the *IPv4 CIDR block* field, enter `10.0.1.0/24` (for private subnet).
5. Click on *Yes, Create*.

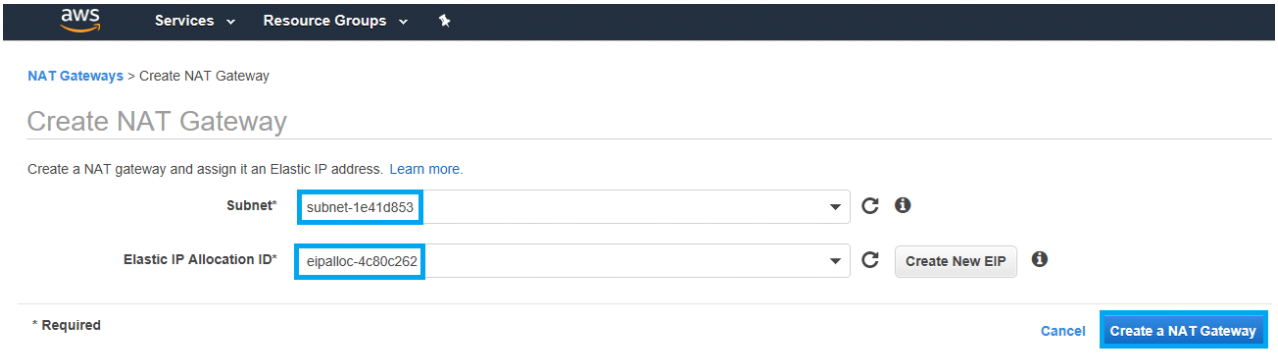
Step 6.2: Create NAT Gateway and set Route Table

The NAT/Internet Gateway for Private subnet is not recommended by AWS security team, and should be temporary for testing and not running real malware

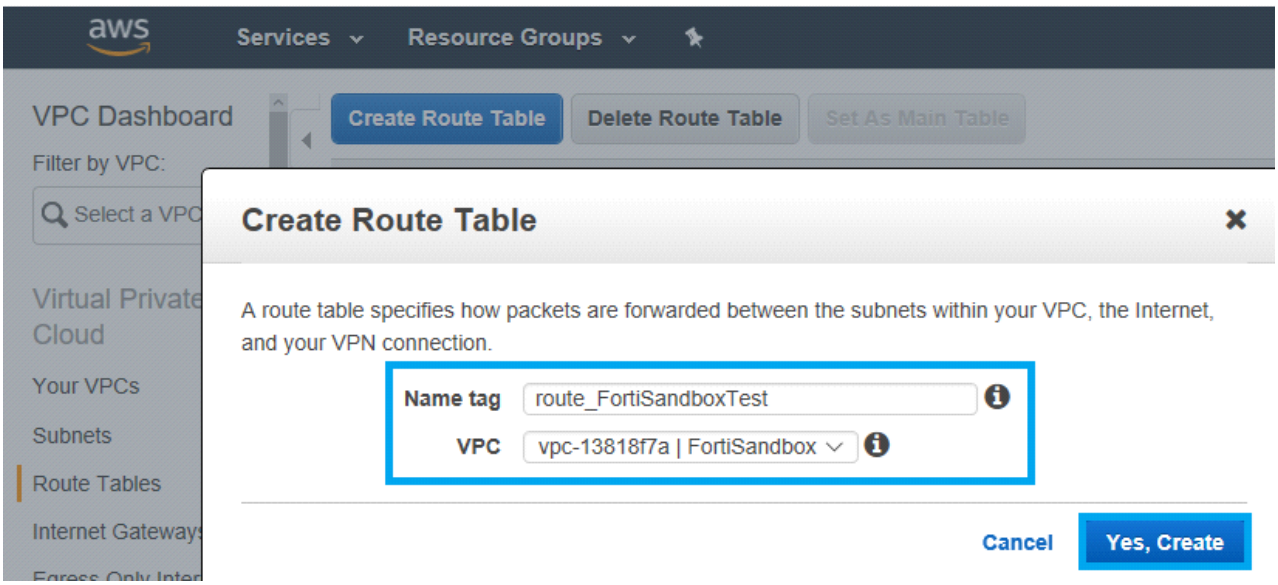
AWS security recommends to use AWS VPN or AWS Direct Connect to route out of an egress point to any third party Internet provider.

To create a NAT Gateway:

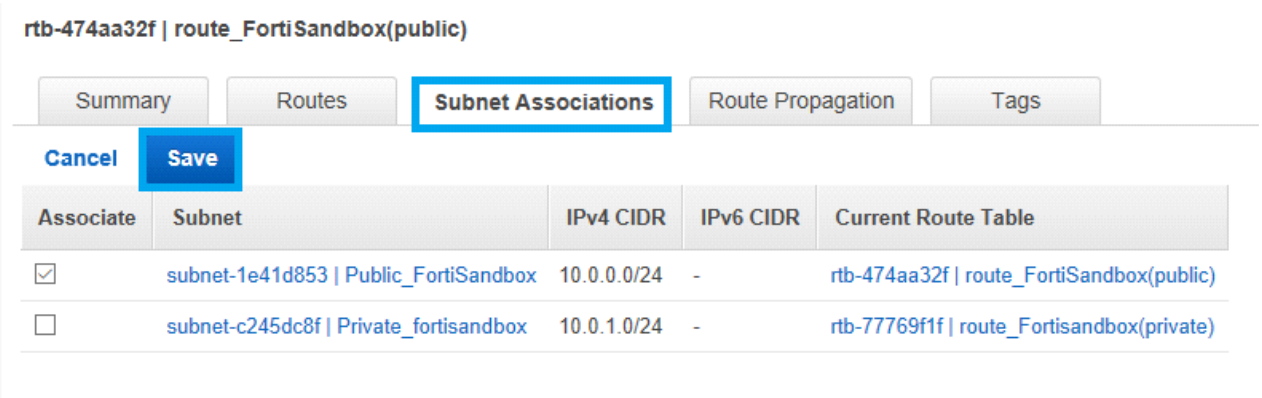
1. Under *Virtual Private Cloud* select *NAT Gateways*.
2. Click *Create NAT Gateway* and select the public subnet you created.
3. Under the *Subnet* drop down, select the *Elastic IP* you created.



4. Click *Create a NAT Gateway*.
5. Under *Virtual Private Cloud* select *Route Tables*.
6. Click *Create Route Table* for the public subnet.
7. In the *Name Tag* field, enter a name.
8. In the *VPC* field, select the VPC you created. Click *Yes, Create*.



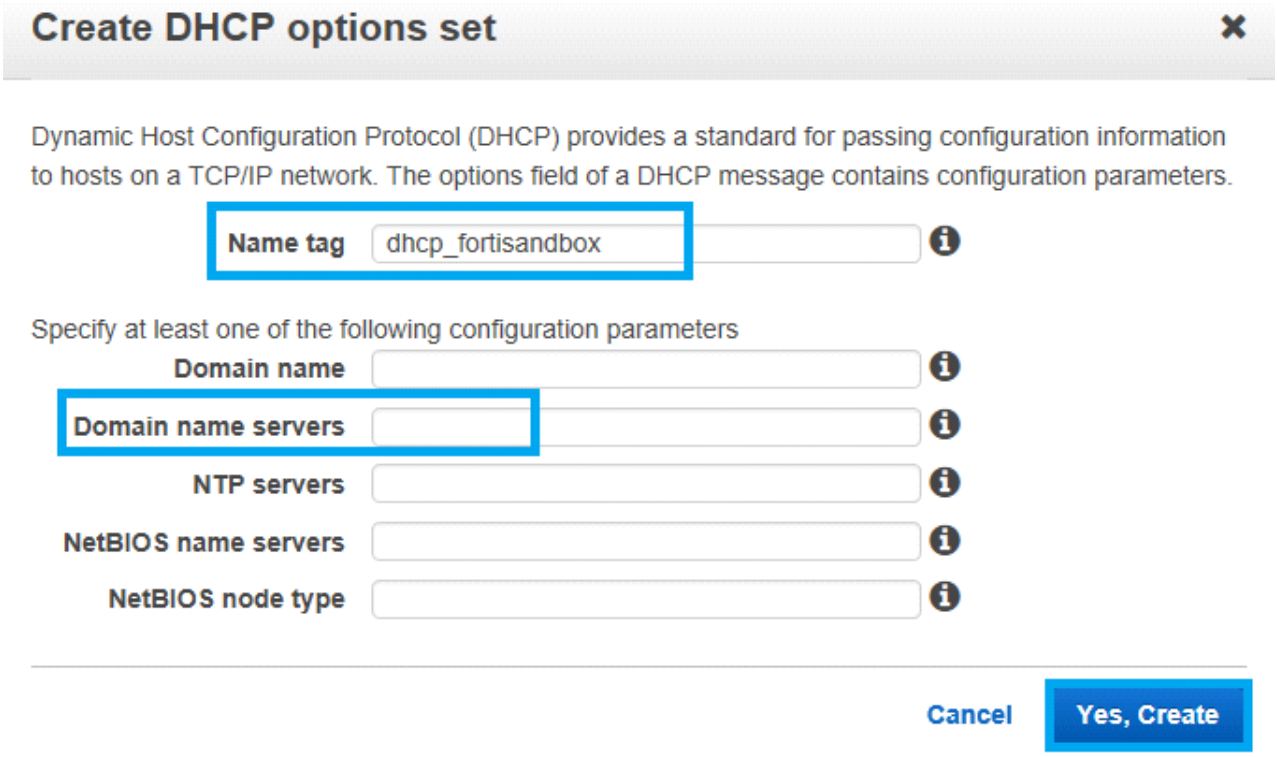
9. Go to *Subnet Associations*.
10. Click *Edit*, select the public subnet, then click *Save*.



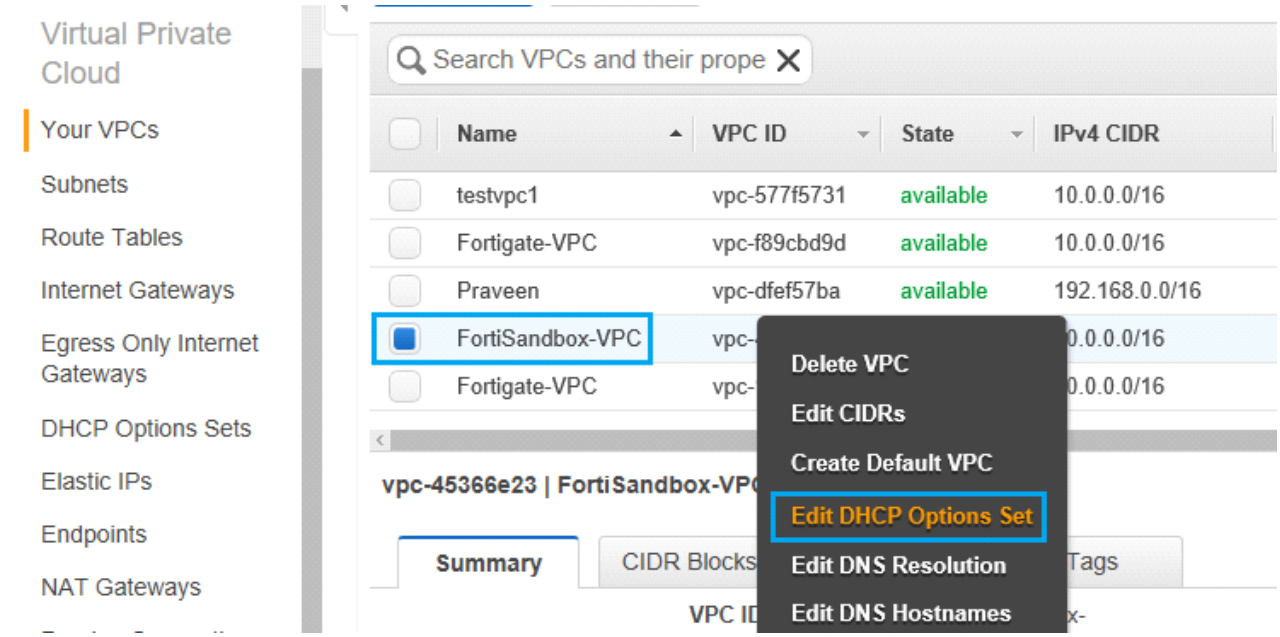
11. Go to Routes, click *Add Another Route*
12. In the *Destination* field, enter `0.0.0.0/0`.
13. In the *Target* field, select the *Internet Gateway* for public subnet you created.
14. Click *Save*.
15. Repeat the steps to create a route table for your private subnet.

Step 6.3: Create and Attach DHCP Options to VPC

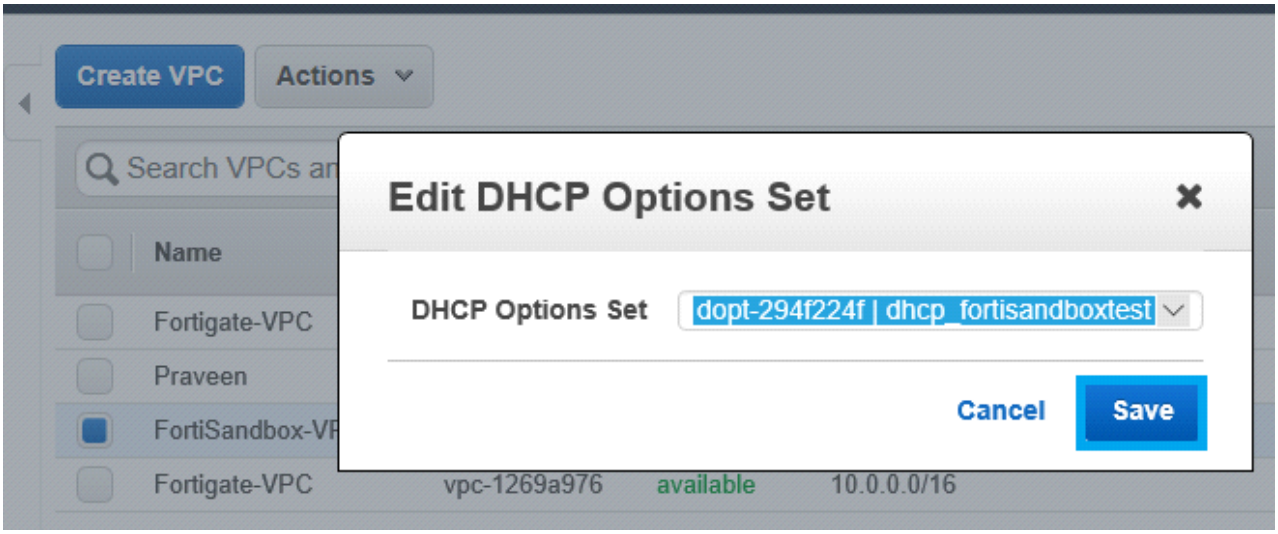
1. Under *Virtual Private Cloud*, select *DHCP Options Sets*.
2. Click *Create DHCP Options Sets*.
3. Under the *Name Tag* field, enter a name. For example, *dhcp_fortisandbox*.
4. In the *Domain Name Servers* field, enter the primary IP address you provided when creating `eth1`. If auto-assigned, enter the IP address from Instance Details.



5. Click *Yes, Create*.
6. Go back to *Your VPCs*. Right click the VPC entry you created and select *Edit DHCP Options Set*.



7. Choose the created DHCP options set and click *Save*.

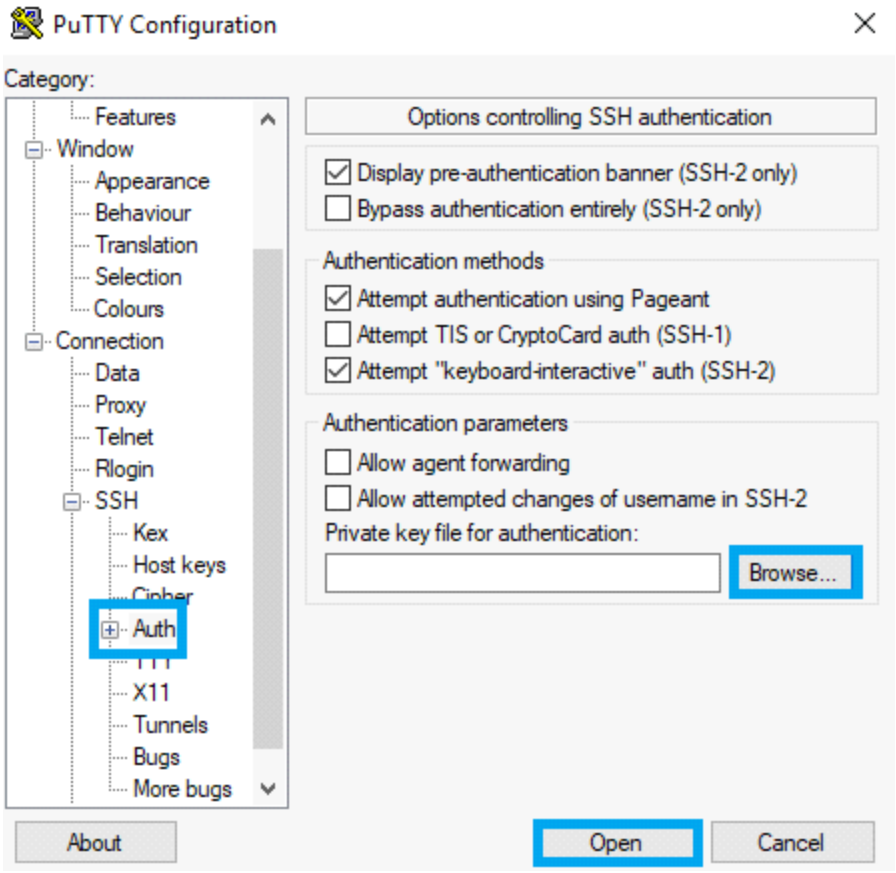


Option A: Install Trial VM

Step 7: Install Trial VM via CLI

If you don't choose the *without key pair* option, log in using password `<InstanceID>`.

1. Before logging in, convert the saved `pem` file which you downloaded while creating the key pair to `ppk` file.
2. Log in to CLI using the *Elastic IP* you created by entering username as admin and with the `ppk` file.



3. In the CLI, run the `status` command to view the VM status.

```
login as: admin
Authenticating with public key "imported-openssh-key"
> status
System:
        Version:              v2.5.0-build0316 (Interim)
        Serial number:
        FSA-VM License:       Valid, 363 day(s) left
        System time:          Fri Oct 27 07:24:11 2017 UTC
        Disk Usage:           5 GB
        Image status check:   OK

        Windows VM:           Initialized
        Disk Size:            31 GB
```

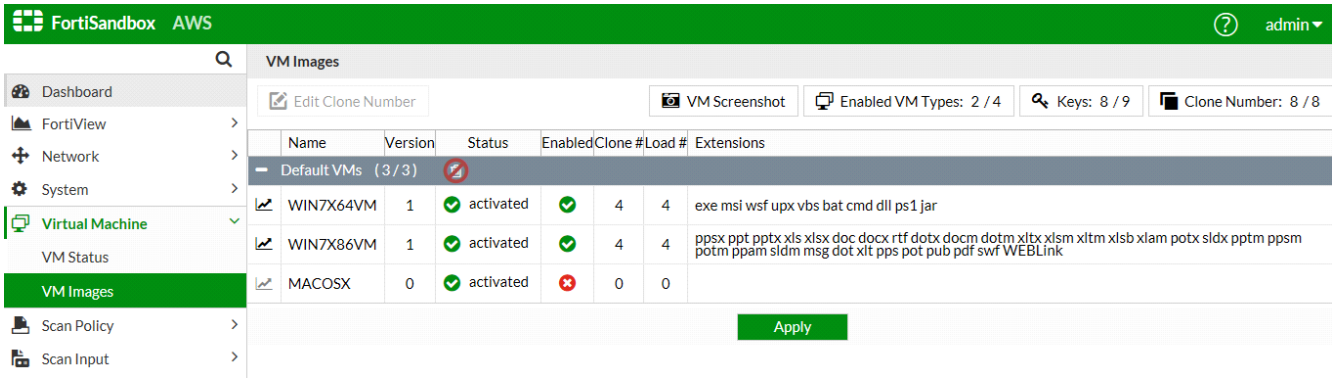
4. Run `installvms`. You should be able to see and configure the VM image clones in the GUI.

```
> installvms
Deploying WIN7X64VM
Downloading vm meta WIN7X64VM
Downloading vm meta WIN7X64VM passed
Downloading vm product list WIN7X64VM
Downloading vm product list WIN7X64VM passed
Downloading package WIN7X64VM
/tmp/aws_vmdir/tmpdlvm.pkg                100%[==============
Downloading package WIN7X64VM passed
Checking sha256
Checking sha256 passed
Unpacking package
Unpack package passed
Installing VM WIN7X64VM
```

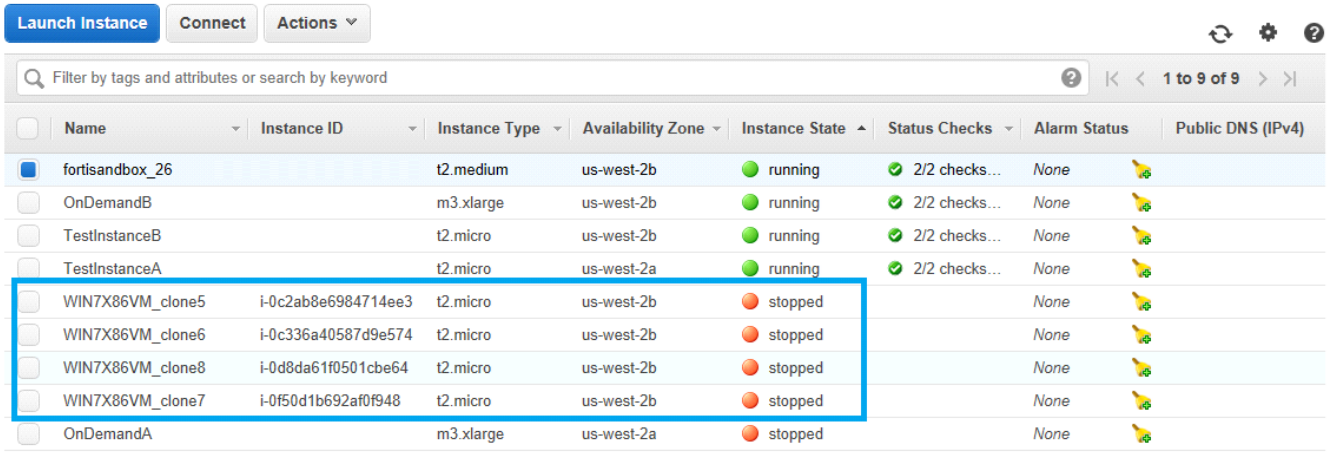
```
Deploying WIN7X86VM
Downloading vm meta WIN7X86VM
Downloading vm meta WIN7X86VM passed
Downloading vm product list WIN7X86VM
Downloading vm product list WIN7X86VM passed
Downloading package WIN7X86VM
/tmp/aws_vmdir/tmpdlvm.pkg                100%[==========
Downloading package WIN7X86VM passed
Checking sha256
Checking sha256 passed
Unpacking package
Unpack package passed
Installing VM WIN7X86VM
```

Step 7.1: Configure Trial VM Clones in Web GUI

After installation in the CLI, go to *Fortisandbox Web GUI > Virtual Machine > VM Images*. You can view installed VMs. If you want to change the clone count, select a clone, click *Edit* the count and click *Apply*.

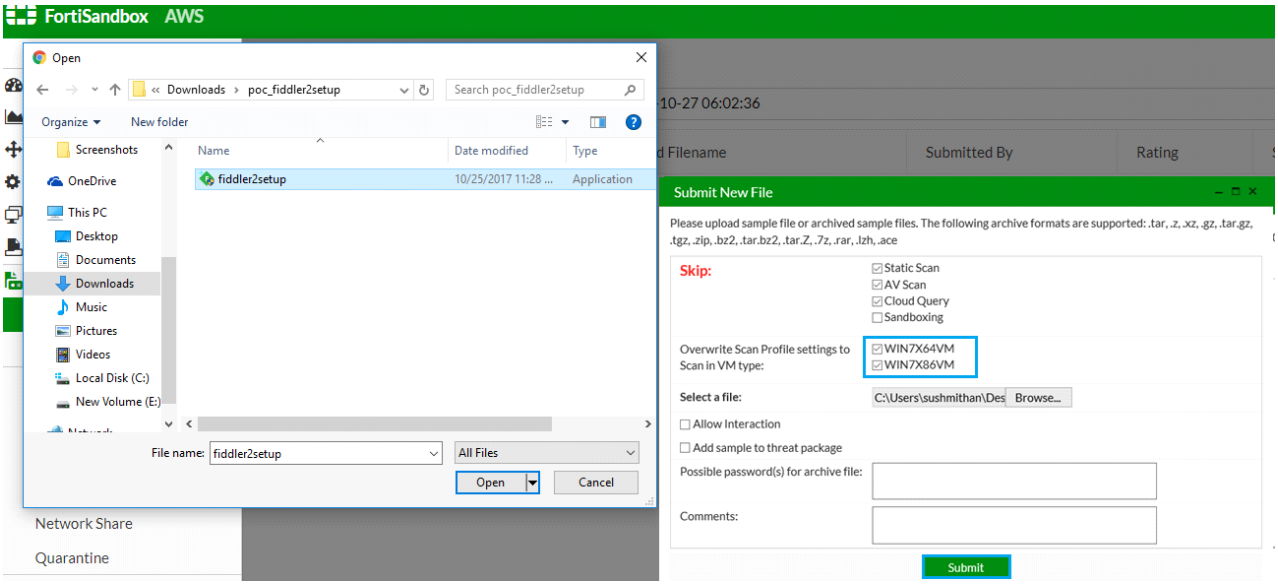


After applying, you can see the launched instance in the AWS console. If you enter four as the Clone count, you can view four instances.



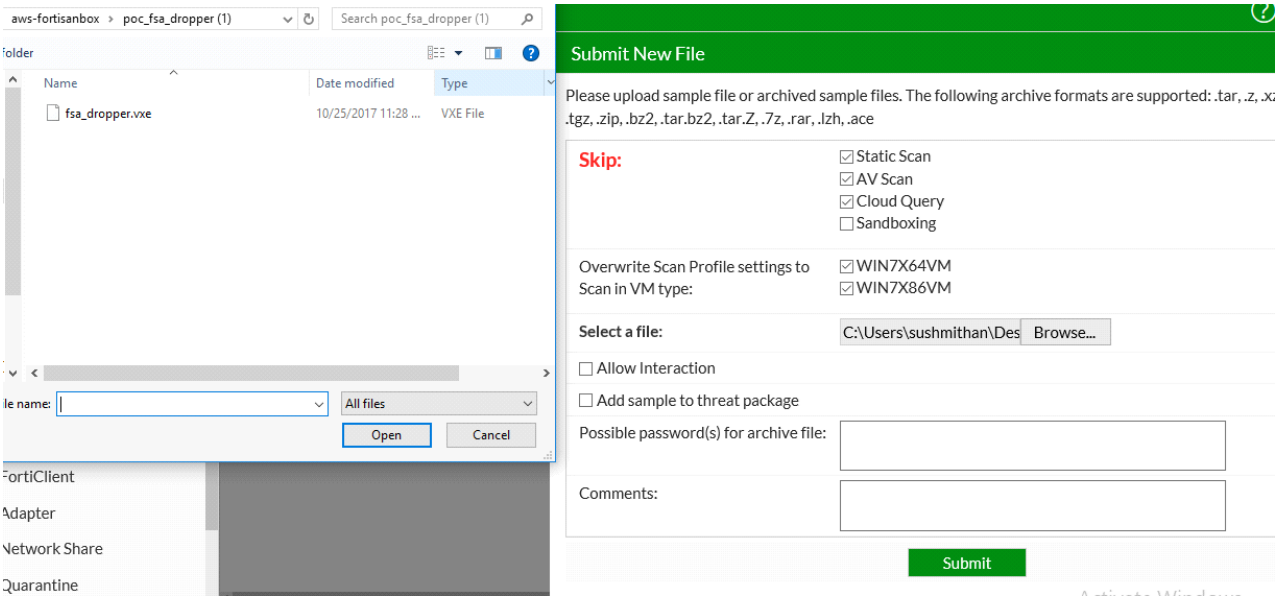
Step 7.2: Submit On-Demand Test

1. Navigate to *Scan Input > File On-Demand > Submit File*. The *Submit File* dialog box will open.
2. Click on choose file and upload the file `fiddler2setup.exe`, and submit. You should receive a *Clean* rating after you send the file to FortiSandbox if the uploaded file is clean and not harmful.



The file `fsa_dropper.vxe`, is a fake high-risk sample created by Fortinet. For harmful malicious behavior, FortiSandbox will detect them as *High Risk*.

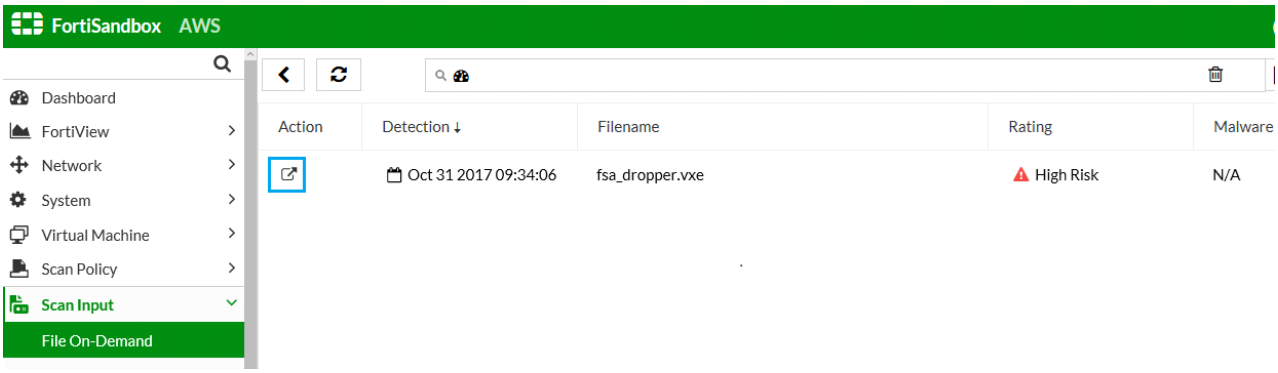
3. Upload any file that might be harmful. For example the `fsa_dropper.vxe` file. Click on *Submit*, you will be alerted by FortiSandbox that this file is harmful if it contains any malware.



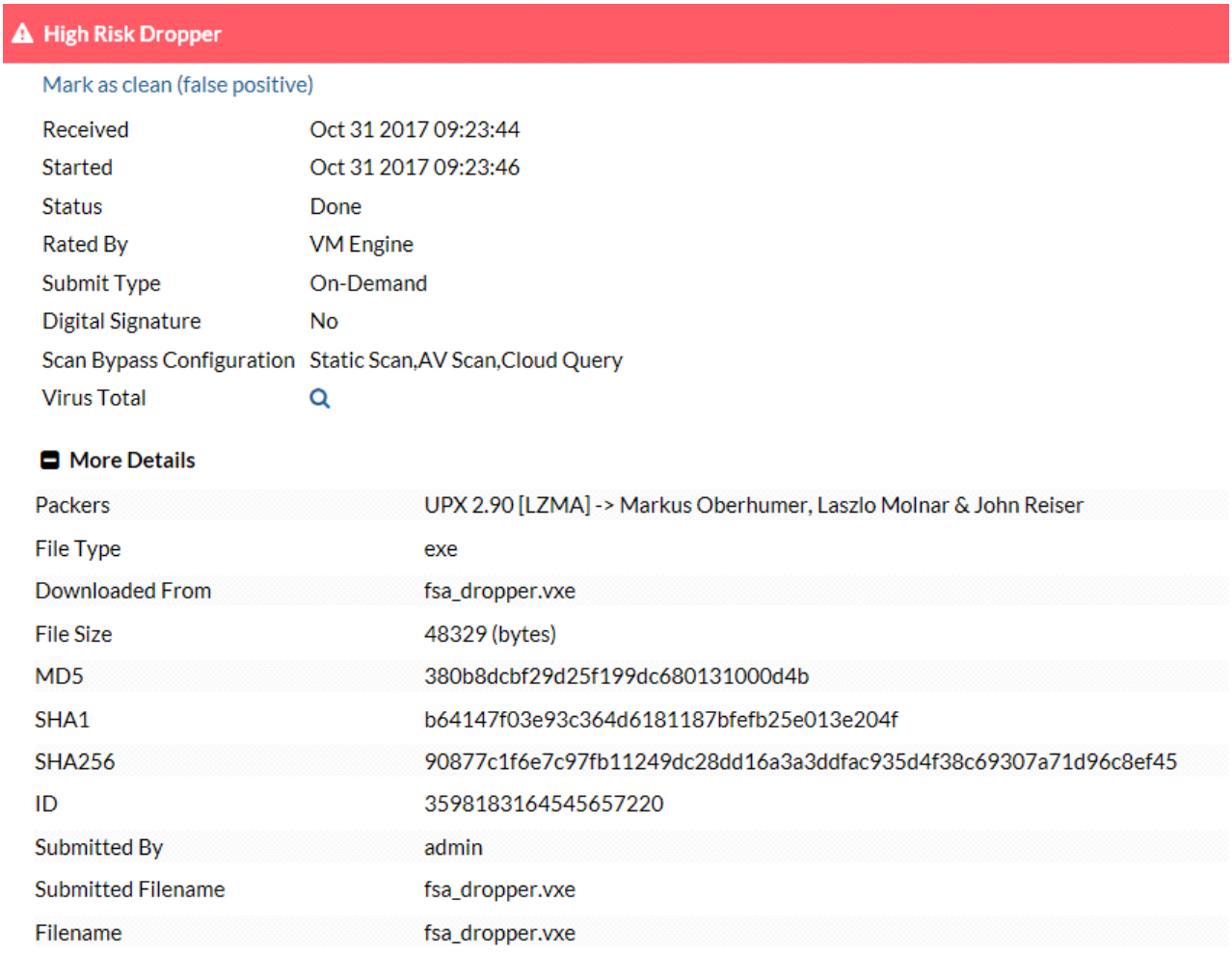
4. After uploading files, you can view *File On-Demand* page and select any file to check.
5. Click the *View File* icon to view its details.

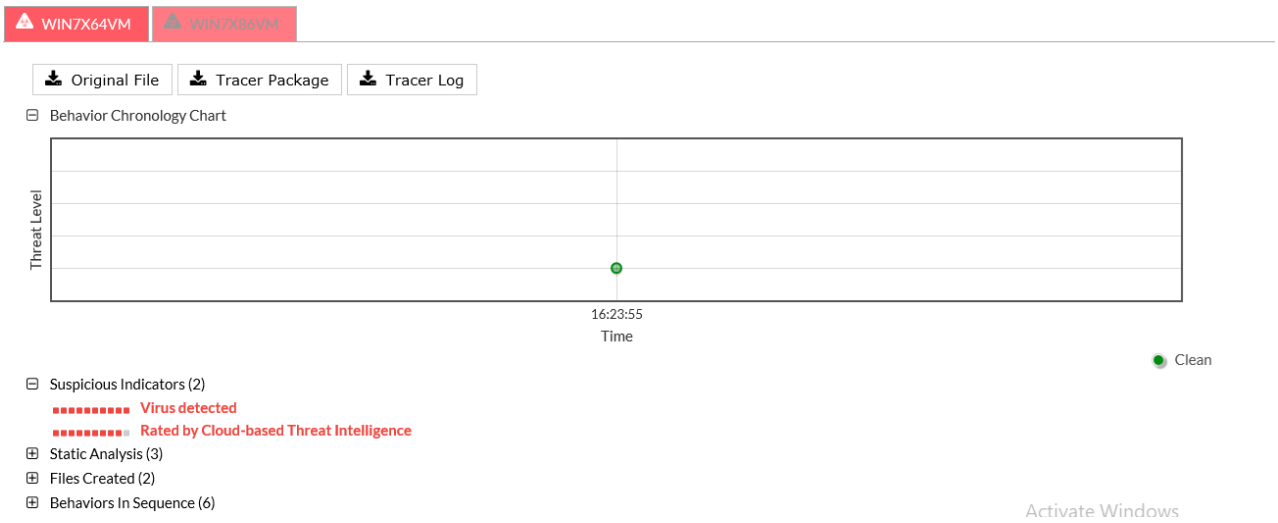
To submit a file for risk analysis:

1. Click on the *View File* icon of the submitted file for risk analysis.
2. Click on the file.



3. Click on *Details*.
4. The *High-Risk Dropper* page will open.




WIN7X64VM
WIN7X86VM
Original File
Tracer Package
Tracer Log
Behavior Chronology Chart
Threat Level
16:23:55
Time
Clean
Suspicious Indicators (2)
Virus detected
Rated by Cloud-based Threat Intelligence
Static Analysis (3)
Files Created (2)
Behaviors In Sequence (6)
Activate Windows

Option B: Install Custom VM

Step 8: Prepare Custom VM

FortiSandbox AWS supports custom VMs. The user can provide the VHD image for created customer VM, and FSA firmware can load the VM image and use it for sample analysis.

How to create a custom VM:

Create the VHD image with a virtualization software solution. For example, VirtualBox. Refer to the custom VM section of the *FortiSandbox Administration Guide* for further details and instruction.

Key components:

- When creating the VM, specify VHD as the disk image format.
- The disk controller must be IDE.
- The disk size must not over 20GB.
- The OS must have the PV Driver installed. (current ver, 7.4.6). https://s3.amazonaws.com/ec2-downloads-windows/Drivers/AWSPVDriverSetup.zip
- Copy the FortiSandbox Tools folder to any location (e. g. `C:\`) of the custom VM, and add the `FSALauncher.exe` to be an auto-startup program. (using the Startup folder or Task Scheduler).
- Windows should be configured to auto-login

Share the VHD file and accessible from SSH/FTP from on public server, or a internal server that can be accessed from the FSA firmware.

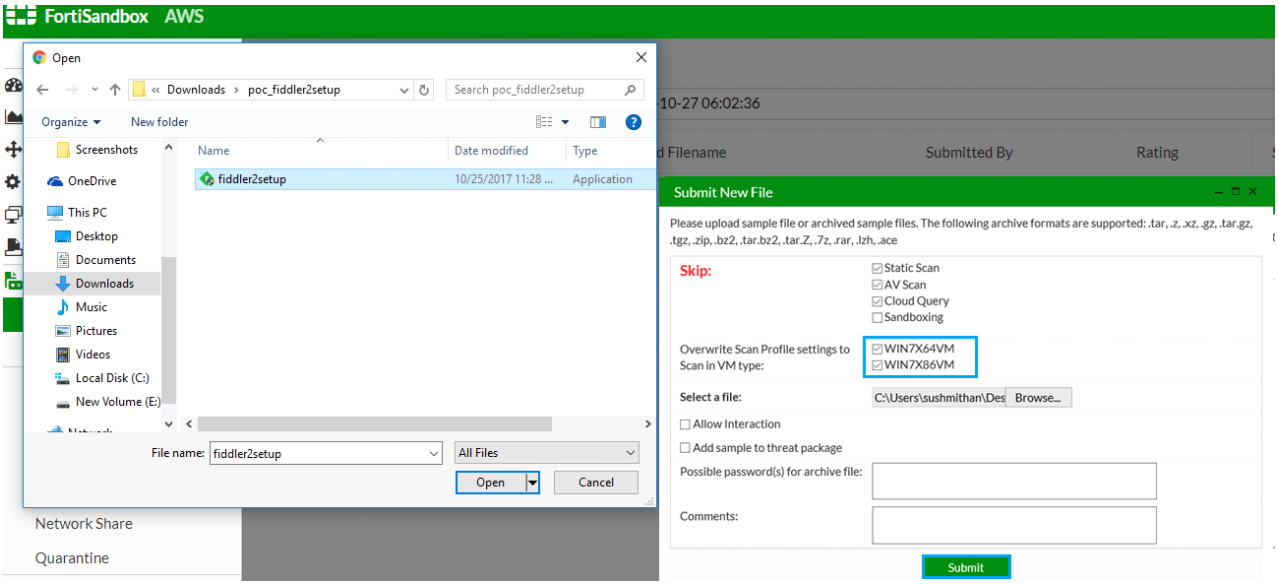
Step 8.1: Install via CLI

1. To install the VM via the CLI, go to FSA firmware CLI.
2. Import the VHD image using CLI command `vm-customized`.

For further information about the vm-customized command. Please refer to the FortiSandbox CLI Reference Guide available in the Fortinet Document Library.

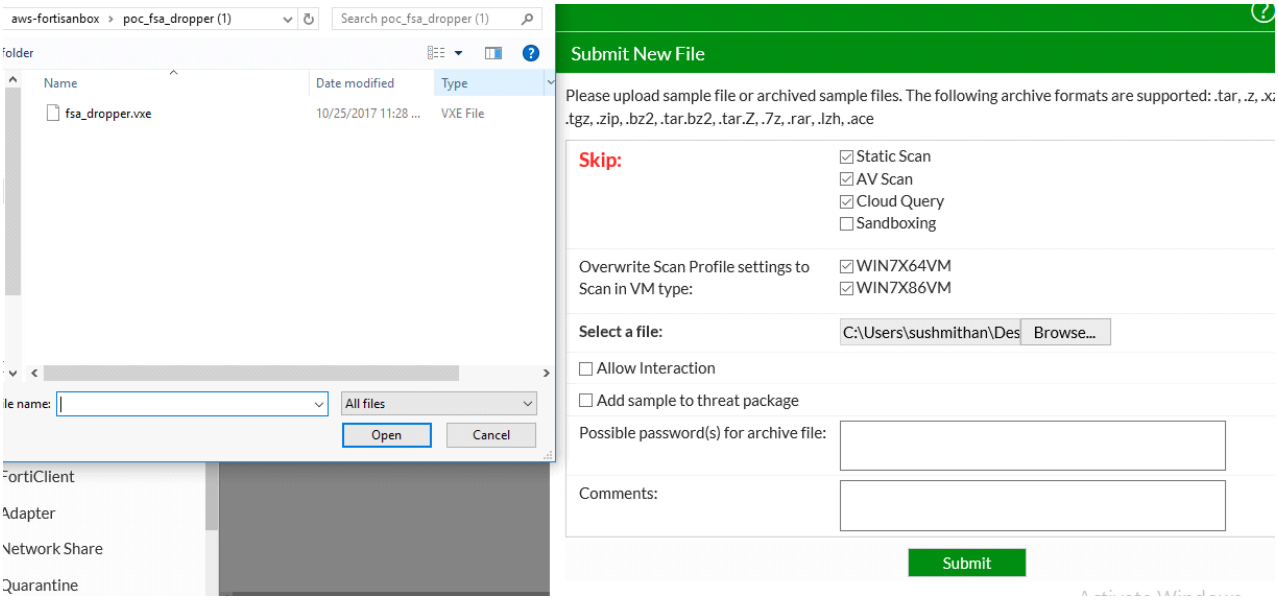
Step 8.2: Submit Test

1. Navigate to *Scan Input* > *File On-Demand* > *Submit File*. The *Submit File* dialog box will open.
2. Click on choose file and upload the file `fiddler2setup.exe`, and submit. You should receive a *Clean* rating after you send the file to FortiSandbox if the uploaded file is clean and not harmful.



The file `fsa_dropper.vxe`, is a fake high-risk sample created by Fortinet. For harmful malicious behavior, FortiSandbox will detect them as *High Risk*.

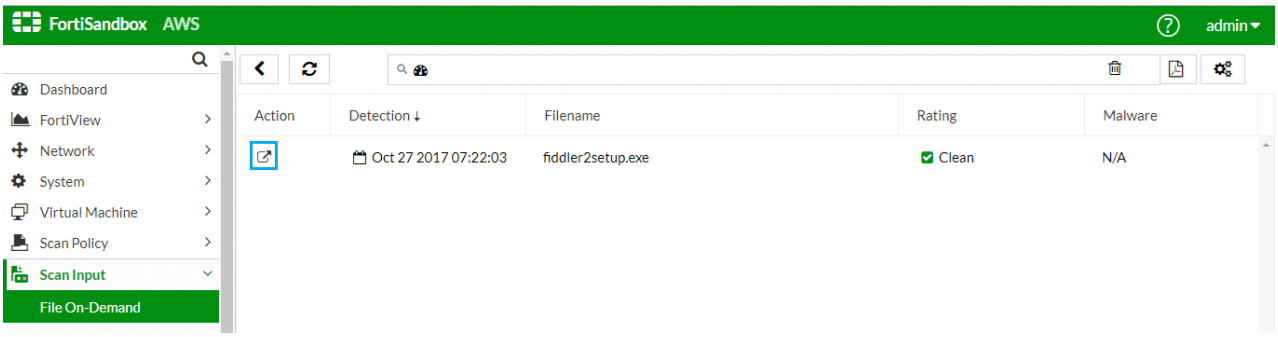
3. Upload any file that might be harmful. For example the `fsa_dropper.vxe` file. Click on *Submit*, you will be alerted by FortiSandbox that this file is harmful if it contains any malware.



4. After uploading files, you can view *File On-Demand* page and select any file to check.
5. Click the *View File* icon to view its details.

To submit a file for risk analysis:

1. Click on the *View File* icon of your submitted file for risk analysis.



2. Click on the file.
3. Click on *Details*.
4. The *High-Risk Dropper* page will open.

High Risk Dropper

Mark as clean (false positive)

Received	Oct 31 2017 09:23:44
Started	Oct 31 2017 09:23:46
Status	Done
Rated By	VM Engine
Submit Type	On-Demand
Digital Signature	No
Scan Bypass Configuration	Static Scan,AV Scan,Cloud Query
Virus Total	

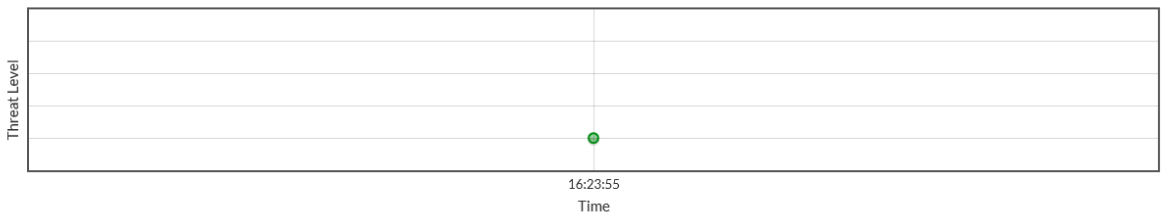
More Details

Packers	UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser
File Type	exe
Downloaded From	fsa_dropper.vxe
File Size	48329 (bytes)
MD5	380b8dcbf29d25f199dc680131000d4b
SHA1	b64147f03e93c364d6181187bfefb25e013e204f
SHA256	90877c1f6e7c97fb11249dc28dd16a3a3ddfac935d4f38c69307a71d96c8ef45
ID	3598183164545657220
Submitted By	admin
Submitted Filename	fsa_dropper.vxe
Filename	fsa_dropper.vxe

WIN7X64VM WIN7X86VM

Original File Tracer Package Tracer Log

Behavior Chronology Chart



Suspicious Indicators (2)
Virus detected
Rated by Cloud-based Threat Intelligence
Static Analysis (3)
Files Created (2)
Behaviors In Sequence (6)

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

Index

S

V